Design and Simulation of Passive Optical Networks (PONs) for Fiber to The Home (FTTH) Applications

C. Charitou¹, N. Stathopoulos²

¹Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications” TEI of Piraeus, Greece, E-mail: bouki21@hotmail.com

²Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications” TEI of Piraeus, Greece, E-mail: nstath@teipir.gr

The continuously increment of the user requirements for telecommunications networks with qualitative and uninterrupted communications led to a tremendous increase in demand for bandwidth and a necessity of upgrading of old technologies. One of the highly promoted technologies for an ultimate broadband internet access is the Fibre to The Home (FTTH) technology. The aim of this paper is to approach the design of a PON, under a set of reasonable requirements for a suburban neighbourhood.

1. Introduction

A Passive Optical Network (PON) is a technology that uses the FTTH technology. A PON uses splitters instead of switches. It’s called P2M Technology, because it shares the bandwidth to all subscribers, i.e. there is no dedication of the optical fibre between the central office and the end user. In a PON, the distance is limited to 10km-20km. The infrastructure of the network affects the number of subscribers will be served. More splits on the network mean less distance [Mohammed A.E.N.A, Rashed A.N.Z., El-Adyad G.E. & Saad A.E.F.A., 2009]. Fibre to the Home (FTTH) [FTTH Council, 2011] is defined as the telecommunication architecture in accordance with a communication path that extends in order to use exclusively optical medium from the CO to the home. So as to be characterized as FTPH, the optical fibre must enter the home, or terminate either on the external wall of the home or no more than 2m.

2. Calculation of coupling coefficients

In the simulation section, we will approach the design of a PON, especially a GPON, under reasonable requirements for a suburban neighbourhood. In the first part we will calculate the power budget along the fibre topology and the access points throughout the passive components, as well as the PON architecture for the required specifications. In the second part we will try to perform the GPON topology using the Optiwave software for optical networks and will exam various scenarios. Figure 1 depicts a GPON optical receiving topology. It consists of a CO and four blocks. Each block has four apartment buildings. The CO is connecting with a star coupler. The blocks (1) to (4) are connected through the couplers (a) to (d) respectively.
The power transfer ratio $R$ of the optical signal from CO up to node 16, which is the worst case, is given by:

$$R_{1-16} = (1-a)^6 \cdot a^2 \cdot \beta^8$$  \hspace{1cm} (1.1)

The total insertion loss is given by

$$L_{\text{min}} = -10 \log_{10} R_{1-16}$$  \hspace{1cm} (1.2)

In order to maximize the $R_{1-16}$ we will find the corresponding coupling coefficient $\alpha$.

The coupling coefficient for the maximization of $R$ will be deduced from the condition

$$\frac{\partial R}{\partial a} = 0 \Rightarrow 2a(1-a)^6 \cdot \beta^8 - 6a^2(1-a)^5 \cdot \beta^8 = 0 \Rightarrow a = 0.25$$  \hspace{1cm} (1.3)

As a result, if the coupling coefficient $\alpha=0.25$ then the maximum optical power will be received at the node (16) and the respective power transmission ratio will be calculated as follows:

$$R_{\text{max}} = (1-0.25)^6 \cdot 0.25^2 \cdot \beta^8 \Rightarrow R_{\text{max}} = 0.01112\beta^8$$  \hspace{1cm} (1.4)

In our topology, the transmitters of the nodes have power=1mW (0dBm) and the receivers are PIN photodiodes with BER=10-15. If the insertion loss of a coupler is 0.1 ($\beta=0.1$db) and minimum power at any receiver is -30dBm, the maximum loss due to couplers should be 0dBm-(-30dBm)=30dB. In order to examine if our topology meets this specification we calculate the losses for the worst case.

$$L_{\text{min}} = -10 \log_{10} R_{\text{max}} \Rightarrow L_{\text{min}} = -10 \log_{10} [(1-a)^6 \cdot a^2 \cdot \beta^8] \Rightarrow$$

$$L_{\text{min}} = -60 \log_{10} [(1-a)] - 20 \log_{10} [a] + 0.8$$  \hspace{1cm} (1.5)

We first examine if our topology meets the specification if $\alpha=0.25$ that we found from the (1.3).

For $\alpha=0.25 \Rightarrow L_{\text{min}}=20.337 \Rightarrow L_{\text{min}} = <30\text{dB}$ Accepted because it meets the spec of maximum loss of 30dB.

Changing successively the coupling coefficient of 0.1 to 0.9 (0<$\alpha$<1) we will identify its values that define the limit that meets this specification.
For $\alpha=0.1 \Rightarrow L_{\text{min}}=23.545 \Rightarrow L_{\text{min}} = <30\text{dB Accepted}$

For $\alpha=0.3 \Rightarrow L_{\text{min}}=20.551 \Rightarrow L_{\text{min}} = <30\text{dB Accepted}$

For $\alpha=0.4 \Rightarrow L_{\text{min}}=22.07 \Rightarrow L_{\text{min}} = <30\text{dB Accepted}$

For $\alpha=0.5 \Rightarrow L_{\text{min}}=24.882 \Rightarrow L_{\text{min}} = <30\text{dB Accepted}$

For $\alpha=0.6 \Rightarrow L_{\text{min}}=29.113 \Rightarrow L_{\text{min}} = <30\text{dB Accepted}$

For $\alpha=0.61 \Rightarrow L_{\text{min}}=29.629 \Rightarrow L_{\text{min}} = <30\text{dB Accepted}$

For $\alpha=0.62 \Rightarrow L_{\text{min}}=30.165 \Rightarrow L_{\text{min}} = >30\text{dB Rejected}$

For $\alpha=0.7 \Rightarrow L_{\text{min}}=35.27 \Rightarrow L_{\text{min}} = >30\text{dB Rejected}$

From the above calculations, we observe that the acceptable coupling coefficient that meets this specification is 0.1 to 0.61, although the maximum optical power transmission ratio is achieved for $\alpha=0.25$. Next, we examine the respective topology for the nodes’ transmitters as is depicted in Figure 2.

![Figure 2: GPON topology (Tx)](image)

The worst case scenario is again the connection of node (16) and as a result the aforementioned calculation procedure is also valid for the transmitters’ topology of Figure 4.

2.1 Simulation

The theoretical calculation concerning the optical power budget along the fibre topology will be evaluated using the OptiWave software. The topology’s simulation scheme is depicted in Figure 3. The couplers 14-16 represent the last block of apartment buildings, where the X coupler_7 is the worst case. Each coupler will have
an additional loss 0.1dB (β=0.1dB). The minimum power at any receiver is -30dBm, thus, the maximum loss due to couplers should be 0dBm-(-30dBm)=30dB. We consider two parameters in our evaluation. The first one is the coupling coefficient (α) in range 0<α<1, and the second one is the length of the fibre (L) with L>0 km (in steps of 0.1km).

We next show the performance for the two parameters. We start the calculation with the coupling coefficient a=0.1 and changing the length of the fibre (in step of 0.1km) in order to define the limit in our topology that meets this specification. The same process will take place for each value of coupling coefficient.

<table>
<thead>
<tr>
<th>Coupling Coefficient=α</th>
<th>Length of optical fibre=L (km)</th>
<th>Optical Power Meter_16 (dBm)</th>
<th>Accepted/Rejected</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>0-0.3</td>
<td>&lt;-30</td>
<td>Accepted</td>
</tr>
<tr>
<td>0.1</td>
<td>&gt;0.4</td>
<td>&gt;-30</td>
<td>Rejected</td>
</tr>
<tr>
<td>0.2</td>
<td>0-0.4</td>
<td>&lt;-30</td>
<td>Accepted</td>
</tr>
<tr>
<td>0.2</td>
<td>&gt;0.5</td>
<td>&gt;-30</td>
<td>Rejected</td>
</tr>
<tr>
<td>0.3</td>
<td>0-0.4</td>
<td>&lt;-30</td>
<td>Accepted</td>
</tr>
<tr>
<td>0.3</td>
<td>&gt;0.5</td>
<td>&gt;-30</td>
<td>Rejected</td>
</tr>
<tr>
<td>0.4</td>
<td>0-0.3</td>
<td>&lt;-30</td>
<td>Accepted</td>
</tr>
<tr>
<td>0.4</td>
<td>&gt;0.4</td>
<td>&gt;-30</td>
<td>Rejected</td>
</tr>
<tr>
<td>0.5</td>
<td>0-0.2</td>
<td>&lt;-30</td>
<td>Accepted</td>
</tr>
<tr>
<td>0.5</td>
<td>&gt;0.3</td>
<td>&gt;-30</td>
<td>Rejected</td>
</tr>
<tr>
<td>0.6</td>
<td>0</td>
<td>&lt;-30</td>
<td>Accepted</td>
</tr>
<tr>
<td>0.6</td>
<td>&gt;0.1</td>
<td>&gt;-30</td>
<td>Rejected</td>
</tr>
<tr>
<td>0.7</td>
<td>&gt;0</td>
<td>&gt;-30</td>
<td>Rejected</td>
</tr>
</tbody>
</table>

Table 1: Accepted and Rejected values
In the Table 1, the accepted and rejected values as a combination between the length=L and the coupling coefficient=α, are tabulated as calculated by the software. It is evident that the maximum margin for length L between the nodes corresponds to a coupling coefficient in the range of 0.2 and 0.3. This result is in agreement with the theoretically calculated value of α for maximum optical power transfer ratio. In particular, the coupling coefficient α for maximum R, will give a margin for insertion loss that may be covered by the fibres between the nodes. If the margin is large enough, then the length of the fibre between the nodes may be increased and the distance between the building blocks may also be increased.

2.2 Study with modulated signals

The topology's simulation scheme is depicted in Figure 4. The frequency of the WDM Transmitters is between 193.1THz and 194.6THz. The characteristics of the MMF and the parameters of the couplers are the same with the topology of scheme. Fabry-Perot Optical Filter are used for selection of the receiver's wavelength. In particular, for channel 16, we determined the filter's centre frequency at 194.6THz. The couplers' insertion loss is 0.1 (β=0.1db) and minimum power at any receiver is -30dBm, consequently the maximum loss due to couplers should be less than 0dBm-(-30dBm)=30dB. We consider two parameters in our evaluation. The first one is the coupling coefficient (α) with values 0<α<1, and the second one is the length of the fibre (L) with L>0 km (in steps of 0.1km).

![Figure 4: Modulated Signal](image)

We next show the optical power performance measurements versus the two parameters. We start the calculations with the coupling coefficient α=0.1 and we change the length of the fibre (in steps of 0.1km) in order to define the Minimum Bit Error Rate (BER). The same process will be followed for each value of coupling coefficient.
In the Table 2, the values as a combination between the length=L and the coupling coefficient=α, are tabulated as calculated by the software. The smaller BER are for coupling coefficient α=0.4 and α=0.5, while for α=0.6 is rejected.

![Table 2: Values of Max. Q Factor and Min. BER](image)

**Table 2: Values of Max. Q Factor and Min. BER**

<table>
<thead>
<tr>
<th>Coupling Coefficient=α</th>
<th>Length of optical fibre=L (km)</th>
<th>Max. Q Factor</th>
<th>Min BER</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>0</td>
<td>106.534</td>
<td>0</td>
</tr>
<tr>
<td>0.1</td>
<td>&gt;0.1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0.2</td>
<td>0</td>
<td>93.0238</td>
<td>0</td>
</tr>
<tr>
<td>0.2</td>
<td>&gt;0.1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0.3</td>
<td>0</td>
<td>56.0794</td>
<td>0</td>
</tr>
<tr>
<td>0.3</td>
<td>&gt;0.1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0.4</td>
<td>0</td>
<td>26.8619</td>
<td>3.06064e-159</td>
</tr>
<tr>
<td>0.4</td>
<td>&gt;0.1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0.5</td>
<td>0</td>
<td>9.58945</td>
<td>4.42776e-022</td>
</tr>
<tr>
<td>0.5</td>
<td>&gt;0.1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0.6</td>
<td>0</td>
<td>2.34259</td>
<td>0.00957519</td>
</tr>
<tr>
<td>0.6</td>
<td>&gt;0.1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0.7</td>
<td>&gt;0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure 5:** For α=0.1 and L=0km, BER=0
Figure 6: For $\alpha=0.4$ and $L=0\text{km}$, $BER=3.06064\times10^{-159}$

Figure 7: For $\alpha=0.5$ and $L=0\text{km}$, $BER=4.42776\times10^{-22}$
3. Conclusion

In this paper presented a design of a PON, especially a GPON, under reasonable requirements for a suburban neighbourhood. In the first part we calculated the coupling coefficients along the fibre topology and the access points throughout the passive components, as well as the PON architecture for the required specifications. In the second part the aforementioned GPON topology was simulated using the OptiWave software for optical networks and various scenarios examined. In order to design a PON that serves a suburban neighbourhood under the required specifications, two basic parameters tested. The first parameter was the coupling coefficient and the other parameter was the length of the fibre. We observed that those two parameters are interrelated. In the second scenario, in the beginning of the scheme we put a WDM Transmitter with 16 outputs connecting to a WDM Mux with 16 inputs and in the end a BER Analyzer. The purpose was to observe for which coupling coefficient $\alpha$ the minimum BER was found.

References


Using information centric networking to support the internet of things

E.N. Gkika¹, C. Patrikakis²

¹ Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: gkikaelinakfika@hotmail.com
² Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: bpatr@teipir.gr

ICN technology, is based on the search of information by its name and not by its location. A “publisher”, publishes the information, where as a “subscriber”, by using an interest packet, announces the request of the particular information. Then, the information is cached and is ready for forwarding to the next node in which might be requested. As a paradigm, a use case is included, which analyzes the use of ICN and IoT technology, for the patients who present problems during their transfer and as a result their constant monitoring even from distance is necessary.

1. Introduction

The use of the internet has become a daily routine necessary to all users regularly, not only to a particular group of people but also to anyone who has a connected on the internet device. Each development throughout the years has created the need for new technologies which will be able to solve the problems created. The use of an increasing number of devices is a daily phenomenon. Each user can own a smart phone, one or more computers but also other devices connected to the internet.

IP has been developed in order to provide a stable and constant connection using end to end communication among the hosts, something which cannot be implemented on mobile networks which constantly change nodes and need a new IP for each change. So, the search of the packet, using IP on a mobile network is very complicated, since through the routing of the packet the search of the packet location must take place.

This process, would be easier by using the architecture based on Named Data Objects (NDOs) or as it is widely known Information Centric Networking (ICN). In this particular technology, the user performs the search on the basis of the objects name, that the internet as it is now, is based on the communication among the hosts.

2. Information – Centric Networking architecture

Information – Centric Networking (ICN), is a new networking architecture which aims to obliterate the problems of the existing architectures (e.x. TCP/IP). The goal of this particular architecture is to shift focus from address-host orient to data - content orient, to stop the point to point dependence and to create “delivery of a named block of data”.

[2]
The users, through ICN architecture, have the choice of requesting data on the basis of the content. “The common principle” that applies, is that there is one publisher, who produces the information and one subscriber, who receives the information. The subscriber shows his interest on the content, the publisher publishes it and then the subscriber receives it automatically. [3]

There are many ICN framework proposals such as, PSIRP, DONA, NetInf. Some of their basic differences, include the way naming occurs and the way in which an object is requested in a content centric approach, based on its name and not its location. Therefore for the user’s security the name of the content requested, must be known. The public key of the provider of that content and the ICN system itself must be able to automatically connect these two – the name of the object to the public key. [2]

4.1. Advantages of ICN

One of the basic advantages that ICN offers is the “efficient distribution of information” and many more mentioned below. Due to an extend request and reproduction of data both P2P networks and Content Distribution Networks (CDNs) operate. Their use creates a tendency for communication based on content where the “Uniform Resource Identifiers (URIs)” and DNs names are used in order to allow the entrance of the copied data in the network. Another positive aspect is that with the particular naming the fact that the bound between name and object can easily be broken is omitted when the object is transferred to another domain. At the same time the placing of the object into another server has as a result an altered form of the objects in the system with the use of another URI.

Security is achieved by using “Transport Layer Security (TLS)” which secures the channel in which communication is established where a basic condition is the mutual trust between user and server. On the contrary in ICN security is achieved in the data, without the intervention of the sender resulting in the integrity of data no matter how many copies may have been created. Another issue that has come to the surface is mobility due to end-to-end connection which creates problems in use and compatibility. ICN does not work with this technology but by sending requests constantly even when there is movement until the appropriate NDO needed be found and can send it to any source that is considered to able to provide services. Last but not least in ICN with the use of in-network-caching, a greater “integrity and performance is provided similar to the data transport networking (DTN)” architecture. [1]

3. ICN Naming

One of the basic ports of ICN design is that it is based on “Named Data Objects (NDO)”. These are independent from their location and the retrieval of data is based on their name which stays the same independently from the location and from how many copies have been created. [1]

There are two basic name classification categories the one that include hierarchical and the one that includes flat. The structure of the first is similar to the form of the names used now, URLs, and the names used are sometimes understandable from the users resulting in being easier for them to perform the search of data they want.
As far as flat names is concerned they are self-certified, sometimes which means that the names are directly connected to the content without the use of Public Key Infrastructure. The process followed for the determination of the name is divided in two categories. The first one is automatic where the name is given on the basis of content where as in the second there is a combination of the sender's public key on the name which with the use of the receiver’s secret key reveals the content. These particular names cannot be read by the users. [1]

4. **Use case: Use of ICN for e – Health services**

The use ICN technology is the most appropriate for the analysis of the e-health use case below. It shows the possibility to have distant communication among devices or even among nodes on move.

According to [4], paper use case is created which refers to the use of ICN technology on a medical model in order to see its function and to evaluate the usefulness of ICN on exchange of medical information among the devices.

This particular use case is the beginning for the development of our example which by using ICN and IoT technologies will be able to provide solutions to patients with mobility problems which makes impossible their transfer to medical centers, to patients suffering from chronic conditions who want to check their vitals even to healthy people who exercise and want to have a general image of their health.

In the above example the device used is a medical device. The particular one used is quite general and anyone can have access to it. In the example analyzed below, in order to make it implemented and easy to use, there is a substitution of “the medical device” with a mobile phone device, something that most people use nowadays but at the same time it is something that anyone can buy with the minimum cost. Moreover, it is a medium which provides security of data through the existing security politics provided by companies of mobile telephony.

4.1. **Naming**

As it was observed in the previous chapters, there are different kinds of naming. In this particular example following the naming chosen by [4], an adjusted naming to the data of the example is created. The hierarchical form of naming, used introduces a “name tree”. Each part from which the name consists of, is a non-defined octacts number providing the “identification of a sub-tree” for that particular name.

Having as a basis a central entity which provides service, the interest packets creates are meant for specific requests and for specific areas. The packets must be small enough in size in order to have space and speed deduction so that the packets must collect the desirable information by using specific sections.

There are four sections used and a general form of the interest packet is:

```
/domin/Searching-service/Sub-category-of-service/Information
```
At first, as it was mentioned before, it is reported that the service will be distributed by the domain which is a specific entity in a certain area, the entities are defined in a specific area with the aim not to use other sections in naming which will report the location. So, when someone sends an interest packet that is reported to the specific area of the entity.

In “Searching-service” section what is searched is determined. The allowed values are:

1. The patients’ name and surname, in Latin characters as referred in his ID or passport, by providing first the surname and after the name. For instance, Papadopoulos Georgios.
2. The “Doctor” variable, reporting the need for doctor search.
3. The “Ambulance” variable, reporting the need for ambulance search in the local area and last but not least,
4. The “Pharmacy” variable for a chemist’s search.

Moreover, as “Sub-category-of-service” specific services which can be provided by a category with the following options are defined.

1. “Measurements” defining that the measurements of the user from the devices must be collected.
2. “Available_Now” for doctor, pharmacies and ambulanced defining that there is need to be immediately available
3. “Available”, when the search is about available services on specific day for certain time period.

The particular section consists of the functions that each service can perform. For example, as far as patients are concerned, their measurements can be send as an interest packet. The supervising doctor sends a packet that when it has to do with the patients, is in order to get the measurements performed by different devices to his mobile phones. So, in this case, the only variable which can follow the patient’s information in the previous section, is “Measurements”. The variables “Available Now” and “Available”, concern only the packets sent by the supervising doctor and are for the search of another doctor in the area, of a pharmacy, or even of an ambulance.

The difference between “Available Now” and “Available” is, that the former is referred to an emergency situation and the need for search of a doctor, or a pharmacy, or an ambulance immediate, whereas the latter, suggest the need for search but without being an emergency. For example, in case of an emergency, with the variable “Available Now”, the immediate need for the use of a doctor who must be present immediately in the patient house or the purchase of medicine which can be vital and needed immediately as well as the search of an ambulance which must be found for the immediate transfer of the patient to the hospital, are mentioned. On the other hand, the use of “Available” variable, is used in case the patient has a problem, which is not that important. The patient may have some increased rates which would be advisable to be checked by a doctor, but without being an emergency.

Furthermore it can be used for the search of a pharmacy which might not be necessary to be visited as soon as possible, just to know which are open late, in order to go as soon as he can. Finally, the use of an ambulance combined to a specific variable, is less used but not unlikely. It can be used in case the patient’s transfer to the hospital is...
not urgent, just for further exams which specific equipment available only to specific hospital, if that is necessary. As a result, the transfer of the patient to the hospital is necessary but not urgent, so, the search of an ambulance, is performed on the basis of each availability.

Priority is given mostly to “Available Now” variable in contrast to “Available”, without meaning that the user who chooses the second one, will wait for long time and will allow the users of first one to be always served first. The requests received in the same time period will form a queue, which will set as a priority the “Available Now” request. When these are served, then the “Available” take turn.

Lastly, in the “Information” section a key word is defined which may be useful during the search. For instance, there may be a request of a patient’s blood sugar or even for all his measurements. Also the doctor’s specialty for example pathologists, cardiologist or even for a specific medication category that must be available to a pharmacy. Moreover, if an ambulance is needed, to check if it is equipped with the necessary equipment until the patient reaches the hospital and if the personal is fully capable.

---

**Figure 1:** Sample of name tree structure.
4.2. Routing and caching

The routing provided focuses mainly on “interest packets”, since the “data messages”, in order to be delivered to the requesting user follow the route that they followed in the beginning; so that each node from which it passes to store the information in order to be ready for forwarding it to the users that will request it. This specific caching is performed on the basis of each caching technique of the node. So, with this technique the spreading has become easier due to the reductions of the servers’ load. In addition, because of the fact that the search is performed by its name, in case there are many users who search the information with specific content, they have the ability to publish their name, through broadcasting it to the network.

For the proper function of what was mentioned before, each NDN node, consists and uses, the “the Content Store (CS)”, which contributes to the storage of the information received, “the Forwarding Information Base (FIB)”, which has similar use with IP FIB and is used for the forwarding of interest packets and last but not least, “the Pending Interest Table (PIT)”, for storage aiming the trace of location that the interest packet had been forwarded the last time.

An interest packet is stored in a “FIB tables” until it reaches the user who has the information requested in his CS. In order to avoid useless interest packets in the network, all NDN routers located in the middle, store the requests in “PIT table”. Finally, when the node which contains the information is found, a copy of corresponding data packet is created in that node returning it back to the one requested it from the same route followed at first. Lastly, a time period in which the packets are considered time out is provided, hence the user can resend the interest packets by establishing proper communication in the network.

4.3. Function

The mobile phone, device will function as an information collector from the devices used for the measurements. These data are stored and sent to each patient’s doctor after his request in order to check the patient’s health.

An example of that particular interest packet is:

/domain/ Papadopoulos_Georgios /Measures/Pressure

The doctor, collects the new data after his request. In case he sees a warning measurement and wants to perform a sort of identification he sends another request of the following form in order to have some older measures:

/domain/ Papadopoulos_Georgios /Measures/Old_Summary

Then, the doctor performs a comparison of measurements. The rates which are stored and can be sent through the user’s mobile phone, are of specific amount, whereas the previous rates are stored in a central server so that they can be always available and easily accessible.
In case the supervising doctor diagnoses a problem by using ICN technology, an interest packet is sent through the mobile phone which searches for an available doctor in a certain area for the particular problem that the patient may have.

The interest packet may be for example as follows:

/domain/Doctor/Available_Now/Pathologist

Or depending on the case it could call for an ambulance by sending an interest packet of the following form:

/domain/Ambulance/Available/Cardiologist

Then, when the doctor finally visits the patient, he receives his medical file through M2M communication. The patient’s mobile phone which has already gathers all the patient’s measurements and has them stored, after the doctor’s request, it sends the data to a relevant device, for example the doctor’s mobile, so that he will be fully aware of the situation.

Finishing with the diagnosis, he suggests a medical treatment that the patient must follow. In order to be supplied with medication a pharmacy must be identified to be located in the area and to be able to provide the category of medication requested. The interest packet sent is of the following form:

/domain/Pharmacy/Available_Now/Anti-pressure

The chemist receives the medical information of the patient with the same process described above or with the traditional way where the patient informs the chemist for any conditions, not only to ensure the necessity of the use of the particular medicine but also to suggest a similar medicine used for the patient’s condition.

4.4. Devices

The devices used for the measurement of the rates vary depending on the conditions and the rates needed. Some devices have been created that gather information mainly in the field of athletics aiming to the check of physical condition. Medical devices and daily used devices connected to the ICN network can provide the information requested.

As far as devices that are available to every home, an example could be an electronic scale, which can measure weight and height and as a result to provide the fat of the user. These information are stored and so by sending an interest packet, the doctor can receive the last rate of the measurement. In addition, an exercising machine, can count and control heart bits under specific pressure conditions in order to check whether the metabolism of the patient works properly by checking the burnt calories on the basis of the kilometers and the time of exercise.

In the case of medical devices, a pacemaker of a heart patient is referred as well as a new contact lenses technology created by Google. In the first case, the heart bit measurements of the patient for the update of his health condition after an open heart surgery and the placing of the pacemaker, can be received for informative purposes. At
the same time, Google has developed a technology which allows through the use of specific contact lenses to check blood sugar by measuring glucose levels through tears1. With the control of the patient directly even through distance and to prevent any changes of the user’s organism which could be fatal.

There are also devices already used in athletics that can be used as they are or adjusted to the data provider. Fitness bands are bracelets created by many companies such as Nike2 (Fuel Band) and Samsung3 (Gear Fit) which allow the collection of measurement from daily activities. They can be used for heart hit rates even in relaxing situations aiming to detect any arrhythmias or pressure increase. In addition as Samsung has already done, to gather sleep data in order to analyze the user’s sleep if he suffers from insomnia, how many hours he is in REM condition, if his sleep is stable and constant.

Last but not least, ICN technology can be incorporate even in training shoes, for example shoes created by Nike which gather measurements which are relevant to the user’s habits. At start there is recognition of activity, walking, jogging, running, cycling and then the steps, the kilometers, the time and the tense in which the exercise was completed are measured4.

Through the specific devices the supervisor doctor can check the course of a patient after a surgery if he follows the instructions for full recovery, if he follows the diet provide or if he does the right exercises on the basis of history. In the devices there is no reason for identification of the location of the user since all the measurements received are gathered through the mobile device which the interest packets.

5. Conclusion

Through a rough analysis of ICN, the conclusion is that it is superior of the already existing network which is used at the moment and it would be very useful in the example of health in distance which has been analyzed. The shift of center of IP to the name and the search of information by using it, has made the use of search much easier mainly in wireless mobile networks. The devices can receive information by searching its name and not by searching the path that must be followed, while the forwarding of the information to multiple users gives the ability of choice to the user who will offer the best possible information, something which provide speed and it is delay tolerant. The route used, is stored for future use. As far as security is concerned, the content is secured and the node of the sender, resulting in integrity and security from possible attacks is also secured.

In the use case used, there is an analysis which proves that ICN technology is more applicable than the use of IP, based on the network. By using ICN technology, there is an interest packet sent, aiming to receive vital measurements, which are necessary for the health monitoring of the patient.

---

1 http://googleblog.blogspot.gr/2014/01/introducing-our-smart-contact-lens.html (assessed on 4th May 2014)
3 http://www.samsung.com/global/microsite/gear/gearfit_features.html (assessed on 4th May 2014)
Acknowledgements

I would like to express my regards to Mr. Patrikaki my supervisor, for the support he provided throughout the thesis. Through conversation, guidance and constant corrections, he helped me to complete my research and at the same time to understand as much as possible the content of the technologies developed. Furthermore, I would like to thanks my family who by financial and psychological support, helped me to reach where I am. As well as my close friends for the constant support in my efforts.

References

Multiband/Wideband Fractal Antennas for Mobile Communications

S. Symeonidis\(^1\), S. Savaidis\(^2\)

\(^1\) Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail:simos421@gmail.com

\(^2\) Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail:ssavaid@teipir.gr

Abstract

The recent technological advances in telecommunications systems are, among others, calling for novel antenna systems that are compact in size and low-profile, yet exhibit broadband or multiband characteristics. Antenna arrays have been used to comply with multi-band or broadband needs, but an ideal antenna element should be able to conform to the outlay of mobile phones and space electronic systems. There has recently been an increasing interest in employing fractal geometry to antenna designs in order to meet the aforementioned desired requirements. This new possibility has opened novel areas of research in both searching fractal antenna shapes and fractal array geometries. In this work a slot loaded fractal antenna is proposed as an optimized outcome of an in house built Genetic Algorithm and an electromagnetic solver with multiband characteristics.

1. Introduction

The increase of demand for antennas due to the constant evolution of wireless communications has led developers to pursue novel design techniques in order to enhance their capabilities and appliances. Some of the most demanding areas for novel applications are aerospace, health, military and every day mobile communications (i.e. cell phones). The last ten years the microprocessors’ evolution has led to smaller devices i.e. smart phones and GPS devices, thus, requiring for the integrated antennas to be equally small. Furthermore, due to the fact that most of the frequency bands are already occupied by multiple applications, the need to explore new spaces in the frequency domain for modern communications arises. These criteria demand from the designers to produce smaller antennas that possess the ability to operate on different frequencies and even more, for some applications, to be multiband or wideband and to conform on different substrate materials without alternating their characteristics. Such antennas are mostly microstrip. There are multiple geometries for microstrip antennas that are being proposed in literature and exhibit the desired characteristics for multiband operation and miniaturization. The most common are fractals, slot loaded and spiral antennas \([1-6]\). Yet several impediments exist such as the selection of frequency of operation according to the user’s specifications, the achievement of the desired amount of reflection coefficient and bandwidth on the frequency of operation and the disability of the user to define multiple desired resonant frequency bands for the radiator. In order to surpass those impediments, many
optimization techniques have been proposed such as neural networks, genetic algorithms and particle swarm optimization [7-13]. This work focuses on the introduction of a new method for the design of microstrip antennas that surpasses the reported disadvantages by creating a hybrid fractal-slot loaded-microstrip multiband antenna receiver via the use of an in house built genetic algorithm (GA) and an electromagnetic solver (EM) as optimization tools.

2. Fractal Antennas

The term fractal literally means broken fragments and was first coined in by Mandelbrot in his infamous work to denote complex shapes that exhibit self-similarity in their geometrical structure [14]. An example is the case of a Sierpinski gasket fractal whose construction procedure is illustrated in Figure 1 [15]. At Stage 0 of Figure 1 there is only an equilateral triangle in black colour that could represent the presence of metal in an antenna shape on a printed circuit board. In Stage 1, a smaller equilateral triangle is removed from the centre of the initial triangle. It is easy to see that in Stage 1 there now are three smaller metallic areas that are a scaled down version of the initial triangle. The procedure is repeated for each of these three triangles and the shape of Stage 2 develops. Each stage of this procedure is named 'iteration'. If the procedure is repeated for infinite iterations, there will appear a shape with a great degree of self-similarity in scale. The connection of this fractal geometry to antenna design engineering is that the black areas in Figure 1.1 may correspond to the metallic areas of a printed antenna.

![Figure 1.1: Construction of a Sierpinski gasket fractal](image-url)
The number of triangles in the Sierpinski gasket are given by:

\[ N = 3^k - 1 \]

\( k \): the number of iterations

For each iteration the new triangle’s sides are 1/2 of the size of the previous iteration triangle’s sides.

This simple principle is becoming increasingly popular in antenna design, and the literature is constantly enriched with novel references of successful antenna designs. We believe that the main reason for the success of fractal antenna geometries lies in two pillars: first, the self-similarity of a fractal shape may be easily manipulated in order to deliver multi-band and wide-band properties in a way that is easier to design compared to Euclidean geometries. Second, a fractal shape inherently exhibits outstandingly long outlines in a small profile area, thus offering the opportunity to design antennas of small size that operate in lower frequencies; this leads to an easier way to implement miniaturized antennas of increased efficiency. Other popular fractal geometries include the Koch curve, the Koch snowflake, the Sierpinski carpet and many more [15].

2.1. The Koch curve

As shown in Figure 1.2, the Koch curve is one of the most well known fractal shapes. Each iteration adds length to the total curve which results in a total length that is 4/3 the length of Koch curve and is given by:

\[ L = \left( \frac{4}{3} \right)^k \]

Here \( k \) is the iteration stage.

\[ \text{Initiator} \]
\[ \text{Length}=1 \]

\[ \text{Generator} \]
\[ \text{Length}=4/3 \]

\[ \text{Level 2} \]
\[ \text{Length}=16/9 \]

\[ \text{Level 3} \]
\[ \text{Length}=64/27 \]

\textbf{Figure 1.2: Koch Curve}
2.2. The Koch Snowflake

The Koch Snowflake is generated using a reversed triangle as the basic function shape, typically it is a closed loop Koch curve and it is the fractal geometry selected for electromagnetic study in this work.

![Figure 1.3: The Koch Snowflake's triangle and its first three iterations](image)

The number of sides after each iteration is increased by a factor of 4, the number of sides after \( n \) iterations is given by:

\[
N_n = N_{n-1} \times 4 = 3 \times 4^n
\]

The length of each side of the snowflake after \( n \) iterations is given by:

\[
S_n = \frac{s_{n-1}}{3} = \frac{s}{3^n}
\]

\( s \): the length of the original triangle

The perimeter of the snowflake after \( n \) iterations is equal to:

\[
P_n = N_n \times S_n
\]

2.3. Sierpinski carpet

The Sierpinski carpet is shown in Figure 1.4; it uses a square instead of the triangle as the basic function shape.
For each iteration, the next generated square is 1/3 of the size of the square of the previous iteration.

Depending on the shape of the original fractal shape generator (e.g. the triangle in Stage 0 of Figure 1.1), the resulting antenna elements can vary with respect to their properties and specifications. Minkowski dipoles/monopoles and Koch monopoles are examples of linear fractal generators [16] [17]. Sierpinski gasket antennas have been also investigated in the literature; it is interesting to point out that there is a Sierpinski-specific iterative analysis of fractal antennas that calculates the antenna's pattern and VSWR based on self-similarity principles rather than employing numerical electromagnetic techniques for each new shape; this results to fast calculations and increased simulation performance [18-30]. Furthermore, fractal tree antennas have been found to exhibit denser multiband behaviour with respect to Sierpinski gasket antennas [21] [22]. It is also interesting to point out that Genetic Algorithms have been employed in the literature and, combined with fractal powerful geometries, have delivered powerful results. The author has used genetic algorithms in antenna designs of Euclidean geometry [23] [24] and it has always been hard to create the initial correspondence relationship between antenna shape and genetic algorithm chromosome. But, fractal antenna shapes are characterized by only a few fractal operators with a limited number of defining parameters, thus making it easy to create powerful genetic representations. Genetic algorithms will be presented in the next section and as reported in literature, when combined with iterative functions systems like fractal geometries can deliver antenna designs of extreme miniaturization and very desirable multiband and radiation properties [25] [26]. For this work the Koch Snowflake was the geometry selected for optimization. This is due to the large area inside the Snowflake making it possible for the application of slots.
3. Genetic Algorithms

Genetic Algorithms (GA) are optimization techniques based on natural selection. Their use is appropriate for the solution of discontinuity, non-linearity and non differentiable multivariate problems. In such algorithms, an initial set of solutions is led gradually to the optimal solution while changing certain characteristics [27]. The interest in the development of genetic algorithms started in the 1960s due to the need for optimization techniques able to imitate nature's mechanisms for the survival and adaptability of species according to their environment. Genetic algorithms were named by Bagley, but John Holland is considered as the inventor who developed them with colleagues and students at the University of Michigan in 1975. Genetic Algorithms possess a number of interesting advantages, such as their efficiency in optimization problems containing both continuous and discrete variables. Furthermore, they don't require information on differentiability and can be simultaneously scan a wide range of solution space [28]. They are also suitable for multivariate problems and can run in parallel computing systems. It is also possible to output multiple optimized variables for a problem, and to function efficiently for numerical and experimental data as well as analytical functions. Last but not least, they have the ability to avoid local maxima or minima [29].

The following table gives a comparison of the method of genetic algorithms with other traditional optimization techniques, the process of convergence of conjugate gradient and the method of random walk.

<table>
<thead>
<tr>
<th></th>
<th>Conjugate gradient</th>
<th>Random walk</th>
<th>Genetic algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall limits</td>
<td>+</td>
<td>++</td>
<td>+++</td>
</tr>
<tr>
<td>Discontinuous fitness function</td>
<td>+</td>
<td>+++</td>
<td>+++</td>
</tr>
<tr>
<td>Underivatized fitness function</td>
<td>+</td>
<td>+++</td>
<td>+++</td>
</tr>
<tr>
<td>Convergence speed</td>
<td>+++</td>
<td>+</td>
<td>++</td>
</tr>
</tbody>
</table>

Table 2.1: Comparison of the method of genetic algorithms with traditional optimization techniques

In this work the objective of the in house built genetic algorithm is to maximize the value of a function that will be presented below (fitness function). The field of the parameter solutions will also be analyzed in the following sections.

1.1. Basic concepts of genetic algorithms and operating principle

Genetic algorithms provide the optimal solution for multivariable problems emulating the operation of natural selection. In the process of natural selection, as in GAs, the fittest organism in the ecosystem gets the higher chance to pass its genetic material to the next generation. Thus the genetic information for successful survival passes to the
next generation of offspring. Through the process of offspring generation (crossover) there is a rare chance for a random mutation. Mutation provides diversity to the ecosystem and in GAs is one of the key concepts to avoid local maxima or minima. After the desired amount of generations, provided by the user, the GA offers the best solution found based on the criteria of the problem [30]. The internal mechanisms of the GA are analyzed below.

1.2. Chromosomes and genes

Each variable used by the GA in order to find its optimal value shall be encoded in the basic structural element called gene. Therefore, the gene is an encoded representation of the parameters of the problem. The length of each gene can be different. The encoding can be done either in the set of real numbers, in binary numbers or in a combination of both [31]. A chromosome is defined as the set of genes that composes an encoded candidate solution for the problem. For example, for the optimization of a radiant device with a microstrip antenna, the variables for optimization are the length L and width W. Choosing binary encoding for the length L and real number encoding for the width in the field of [5 15], some candidate chromosomes and therefore candidate solutions for the problem should be:

Chromosome 1: [0111, 10]
Chromosome 1: [1011, 6]
Chromosome 1: [1001, 12]

1.3. Population and generation

A Population is defined as a set of chromosomes. Inside the population, different chromosomes are reproduced through crossover operators and sometimes are being mutated through mutation operators in order to generate new chromosomes. Thus by this process the most suitable breeding parent chromosomes transfer genetic material into offspring chromosomes that constitute a new group called generation. When the initial population has been replaced by the new, the process is repeated until an optimal solution is found.

1.4. Parents and children

The initial population of chromosomes which are involved in the replication process are called parents. Their selection is based primarily on their suitability to be optimal solutions and it is achieved through several techniques, such as the roulette method and tournament selection that will be analyzed below. The new chromosomes created possess the genetic material of both parents and are called children or offspring. The children chromosomes will replace the previous generation creating a new generation with better features thus leading the problem closer to the optimal solution.
1.5. **Fitness Function**

The fitness function represents one of the most important aspects of the GA. It provides a value to each chromosome that represents their suitability to be the optimal solution. Thus, the higher the value given by the fitness function, the closer for the chromosome is to be the optimal solution to the problem.

The following steps describe the mechanism in which the GA concludes to the optimal solution.

1) Coding the solution space, i.e. the variables of the problem, in genes, construction of chromosomes and construction of the original population (initialize population)
2) Calculate the value of the fitness function for each member of the population
3) Select parents
4) Conduct crossover
5) Conduct mutation operations and create the new generation
6) Replace the old population with the new and repeat the procedure from step 2 if the termination criterion is not reached.

Once the termination criteria are satisfied, the procedure stops and the optimal solution has been found. Schematically, the above procedure is as follows:

![Flowchart of Simple Genetic Algorithm](image)

*Figure 2.1: Implementation of simple genetic algorithm*
1.6. Selection operators

As shown in Figure 2.1, the optimization using genetic algorithms is based on chromosomes with appropriate characteristics, in each population, in order to convey their genes to their offspring and establish a stronger population with better characteristics than the previous, until the optimal solution is reached. For the choice of parents, a set of techniques was developed, some of which are stochastic while other deterministic [32]. The selection is based on mechanisms that combine the value of fitness function of each chromosome and the mean fitness function of the complete population so that local maximums to be avoided.

4. The application of the in-house built Genetic Algorithm for the optimization of the fractal antenna

In our GA, the first 20 genes of the chromosome vector were related to the shape of the slots inside the radiator. Their representation was in binary form. This vector was turned into a 5x4 table that constituted the upper left part of the Cartesian plane radiator and then it was mirrored to the other three parts of the Cartesian plane that provided the required symmetry in both x and y axes for the creation of the radiator. The fractal microstrip was set to be a perfect conductor. The 21st gene represented the size of the radiator's slots W (width) and L (length). W and L were set to be equal. Finally, the 22th gene represents the position of the feed on the axis Y.

[1] Results of simulations

In this section the results of the optimization obtained from the design of a fractal - slot loaded microstrip element using the theory of the three previous chapters will be presented. The desired resonant frequency bands for the optimized antenna were between 800 MHz and 4 GHz.

[2] The initial fractal geometry

The initial fractal geometry used in the experiment was a Koch Snowflake. As shown in figure 3.1, the third iteration of the Snowflake was selected in order to be optimized. It was founded that the bandwidth capabilities of the fractal were limited before the selected iteration and the computational power required was great at the next iteration. Therefore, in the third iteration, a trade off exists between bandwidth and computational power. Possible resonant frequency bands for this antenna were scanned in the space between 800 MHz and 4 GHz through multiple setups. Along the optimization procedure, the dimensions of the conductor were the same as the initial geometry, 18x16cm.
The reflection coefficient of the antenna, as shown in Figure 3.2 had an S11 of -7.8db at 3.5GHz. The main purpose after the implementation of the genetic algorithm was to create an antenna with a reflection coefficient less than -10db for the first band of operation and to possess multiband characteristics by resonating in at least two frequency bands greater than the first.

[3] The implementation of the GA to the initial fractal geometry

The Matlab script of the fitness function for the implementation of the GA in the initial fractal geometry for the absolute value of the S11 that was simulated in HFSS for each radiator was:

```
if (S11 <30)
    A = A + 4. * ((30-S11) ./30). ^ 2;
end
```
val = 1 / (1 + (A ^ 0.5)); % Calculation of fitness function value

A: The additive error
val: The value of the fitness function for each radiator between 0 to 1

The fitness function was set to provide the best values for antennas with a reflection coefficient near -30 db for the desired frequency of operation. The type of the GA’s chromosomes representation was chosen to be binary and the crossover and mutation operations were applied deterministically. As a selection operator, the normalized geometric calibration was implemented with a value of q = 0.08. The crossover operators used in the experiment were arithmetic, heuristic and simple crossover. For the mutation, uniform and non-uniform operators were chosen. The number of population was set to be 60 chromosomes and the number of generations was 120.

[4] The implementation of the GA

For the implementation of the GA the frequency of optimization was set to be at 1 GHz. Furthermore, two more setups were selected at 3GHz and 3.5GHz in order to be optimized as additional resonant frequency bands. Figure 3.3 shows the geometry of the antenna and Figure 3.4 the S11. The black dot in Fig. 3.3 indicates the position of the feed.

![Figure 3.3: The slot loaded fractal geometry](image)
As shown in Figure 3.4, the S11 of the antenna at 1 GHz is -17.5 db. Furthermore, the other two frequency bands selected for optimization exhibit an S11 of -7.5db for 3GHz and 3.5GHz.

As shown in Figure 3.5 the value of the fitness function increases as the generated antennas mach the desired criteria, the maximum value of the fitness at the end of the 120th generation is 0.95 and the best chromosome found is:

\[ \text{Ch} = [0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0] \]

The size of each slot created was 7.23x7.23 mm and the position of the probe was at (0, 6.293) of the x,y axis.

This antenna has shown to deliver promising results for multiband operation. Due to the limiting resources of the computational unit, it has not been possible to further
improve the operation for multiple lower or higher resonating frequencies. For better manipulation of the proposed optimization tool's capabilities, a cluster computer unit is desirable. This will eliminate the need for RAM memory and core processors that are required for the calculation of the S11 in such complex geometries, thus the estimated time for optimization will be limited to several hours.

5. Conclusion

In this work, an in house optimization tool based on MATLAB and HFSS for the development of slot loaded fractal antennas that resonate according to user defined criteria is proposed. Using the theory described in the first three chapters, a Koch Snowflake fractal antenna was optimized by creating slots on its inside geometry. The two antennas presented in Chapter four have been shown to provide promising results concerning the optimization of multiband slot loaded fractals operating to the desired frequency bands. Yet, the computational power required in order for the GA to generate the desirable solutions in such complex geometries is great. Thus with more advanced computational units it is possible to achieve better results with greater flexibility among frequencies of operation via the in-house built optimization tool.

References


Adaptive real time video streaming over satellite

I. Tampakakis\textsuperscript{1}, D. Adamopoulos\textsuperscript{2}

\textsuperscript{1} Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: giannis_tabakakis@hotmail.com

\textsuperscript{2} Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: dxa@otenet.gr

Implementing a real time video streaming system in unstable telecommunication environment such as satellite communication systems, demands specific technologies and tools. H.264 SVC (Scalable Video Coding) is a codec that can enable video streaming over satellite. Moreover, RTSP (Real Time Transfer Protocol) RTP (Real Time Protocol) and RTCP (Real Time Control Protocol) have proved that are sensible for real time video transferring. An adaptive system that can efficiently transfer real time video stream over satellite was designed, created and tested in this thesis project. Results showed that system can be effectively used in satellite environment and is able to change the bit rate depending on the packet loss rate of the channel.

1. Introduction

Satellite communication systems are being developed day by day and are applied to various systems all over the world. The most important advantage that a satellite communication system provides, in contrast with other telecommunication systems, is the wide area coverage. It is true that real time video streaming applications are used by many people all over the world in daily basis. Current satellite technologies are capable of providing enough bandwidth for efficient real time video streaming but only by using specific technologies and tools.

In the current project, a system that will enable real time video transferring over satellite channel will be implemented by using Java language and applet technology. The benefits derived from the project are multiple. The most important benefit is that efficient video transferring in such environment will be enabled. Also, the use of applet technology does not require any installed application in the device of the user, but only the activation of Java in the browser making the procedure easier. Moreover, Java is a cross-platform language which makes the system that will be developed platform-independent.

2. Video streaming over satellite

In order for the reader to understand real time video streaming, video streaming over satellite must be explained.
2.1. Video Streaming

There are two main forms of video streaming over the internet, the transfer of a real time video and the transfer of a stored video. Apostolopoulos et al. (2002) mentioned that for video streaming there are many forms and properties that should be considered. In the next table these parameters are presented and are also selected for the current project.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Current project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point-to-point, multicast or broadcast</td>
<td>Refers to the receiver(s)</td>
<td>Point-to-point communication</td>
</tr>
<tr>
<td>Real time encoding or pre-encoded video</td>
<td>Videos can be pre-encoded or real time encoded</td>
<td>Real time encoding</td>
</tr>
<tr>
<td>Interactive or non-interactive</td>
<td>Refers to maximum accepted video delivery delay</td>
<td>Non-interactive</td>
</tr>
<tr>
<td>Static or dynamic channels</td>
<td>Refers to bandwidth, delay and packet loss</td>
<td>Dynamic channel</td>
</tr>
<tr>
<td>Constant bit rate or Variable bit rate channel</td>
<td>Channel bit rate</td>
<td>Variable bit rate channel</td>
</tr>
<tr>
<td>Packet switched or circuit switched</td>
<td>Type of network</td>
<td>Packet switched</td>
</tr>
<tr>
<td>QoS</td>
<td>Available quality of service</td>
<td>Non available QoS</td>
</tr>
</tbody>
</table>

*Table 1: Video streaming properties.*

2.2. Video coding

Before transmitting any video over a network, the user should compress it in order to reduce the size and achieve transmission efficiency. There are two main categories for video coding: the scalable and the non-scalable coding. Scalable coding can change the transmission bit rate while non-scalable has one specific constant bit rate available.

There are multiple video coding standards designed mainly by ITU (International Telecommunication Union), MPEG (Moving Picture Experts Group) and the Joint ITU/MPEG group. The main ITU standards are the H.261 and H.263. The main MPEG standards are the MPEG-1 and the MPEG-4. The main joint ITU/MPEG standards are the H.262/MPEG-2 and the H.264/MPEG-4 AVC.

Wiegand et al 2003 have made a comparison research for some of the main coding standards (MPEG-2, H.263, MPEG-4 and H.264/AVC). They proved that H.264/AVC codec performs better at any given bit rate. The results are presented in the next figure.
For adding scalability to H.264/AVC, the ITU with MPEG standardized a scalable extension, called SVC (Scalable Video Coding) which removes some parts of the video in order to reduce the bit rate without damaging the video.

2.3. Video streaming protocols

Video streaming protocols can be split depending on the OSI layer to which the protocol belongs. Consequently, there are three main categories for streaming protocols.

Network-layer protocol (IP), provides basic network addressing for video streaming over the internet.

Transport-layer protocol includes TCP (Transmission Control Protocol), UDP (User Datagram Protocol), RTP (Real Time protocol) and RTCP (Real Time Control Protocol). RTP and RTCP are operating on the top of TCP and UDP. RTP has been designed for real time applications while RTCP are used for providing QoS control of the RTP session.

Session-layer protocol defines procedural control messages during the established session. Such messages could cause, for example, the start or the end of a video stream. The most common protocols for such operations are the SIP (Session Initiation Protocol) and the RTSP (Real Time Streaming Protocol).

2.4. Satellite communications and video streaming

Satellite communications are providing connectivity worldwide. Moreover, they are able to connect users in places where no other communications are available (such as mobile etc.).

At the other hand, satellite communication systems are significantly affected by weather conditions like rain, clouds, fog, tropospheric scintillation or gaseous absorption (CHRONOPOULOS, Spyridon K. et al.). Moreover, the network delay due to the distance with the satellite, the high average of packet loss, the jitter effect and the low available bandwidth, are adding extra difficulties at the use of new applications.
Few satellite systems are used today for video transferring. Most of them are broadcasting data and are used for one way communication. The main satellite technology for broadcasting video is the satellite TV. The main satellite technology that can efficiently transfer video (both ways) is the VSAT (Very Small Aperture Terminal).

Further to above paragraph, H.264/AVC SVC coding standard seems to be more appropriate for the designed application, as it can operate in low bit rates as well, and keeps the quality at better levels than other coding standards. Also, since TCP adds important delays due to retransmissions and UDP does not guarantee packet delivery, RTP with RTCP seem to be more capable of handling the real time video application that will be implemented. What's more, RTSP is used in most of the video streaming servers and was designed to manage data streams.

3. H.264 SVC: Analysis, modeling and implementation

This chapter is the multimedia communications part of this thesis project. As presented in a previous chapter, the scalable extension of MPEG4/H.264 AVC (Advanced Video Coding) seems to be more appropriate for use in satellite environment. This extension is called SVC (Scalable Video Coding) and will be the subject of the study in this chapter.

3.1. The H.264/AVC standard

The H.264/AVC (Advanced Video Coding) standard contains two major layers, the Network Abstraction Layer (NAL) which provides network header information for the transferred video and the Video Coding Layer (VCL) for video content representation. H.264/AVC standard organizes the frames into GOPs (Group of Picture). Also, in H.264/AVC like in most of the codecs, picture is separated in macro-blocks. Each macro-block contains 16x16 fixed luma sample and two 8x8 of the corresponding chroma samples. A typical encoding/decoding procedure is presented below.

![Figure 2: H.264/AVC encoding procedure.](image)

Macro-blocks are organized into slices which are parts of a picture that can be decoded independently. Each picture has one or more slices and each slice is independent from the other slices. They are mostly used by H.264 encoders for error resilience, generating accurate to MTU (Maximum Transmit Unit) payloads, and simultaneous processing because they are independent to each other. There are five different slice types.

$I$-Slice: All macro-blocks are coded using intra-prediction technique. $P$-Slice: Each macro-block is inter-predicted with one MCP (Motion Compensation Prediction) signal
per block. **B-Slice**: Each macro-block is inter-predicted using the average of two MCP (Motion Compensation Prediction) signals per block. **SP and SI slices** are the new proposed slices by H.264/AVC and they are beyond the scope of the current research.

H.264/AVC contains 3 different profiles. The **baseline** profile contains low computational costs and coding efficiency by supporting I and P slices, CAVLC coding (Context Adaptive Video Length Coding) and optionally SP and SI slices. The **main** profile targets only in coding efficiency and supports the same features as baseline, but additionally supports B slices and CABAC (Context Adapting Binary Arithmetic Coding) algorithm. At last, **extended** profile supports all the above features except from CABAC algorithm. In this research, baseline profile will be implemented. That means that the main features that should be implemented will be the following.

- **I and P frame prediction**: For I frames intra-picture prediction will be used while for P frames inter-picture prediction will be implemented.
- **Discrete Cosine Transform**: A two-dimension 4x4 discrete cosine transform will be implemented for each of the macro-blocks.
- **Quantization**: Each transform coefficient will be quantized using a quantization step.
- **Entropy Coding**: The quantized macro-blocks will be entropy coded using CAVLC algorithm.

### 3.2. The H.264/AVC SVC extension

SVC (Scalable Video Coding) extension of the H.264/AVC standard has been created in order to change the coding bit rate so as to be able to perform better in lossy environments like satellite communications. SVC provides three different scalability types, temporal, spatial and quality or combinations of those three types (SCHWARZ, Heiko et al., 2007).

Temporal scalability is provided by splitting the bit stream into temporal base layer bit stream and temporal enhancement layer bit stream. Spatial scalability is generating different spatial resolution for each frame and is beyond of the scope of this project. In Quality scalability the video encoding quality is the trade-off for reducing the transmitted data. There are three different quality scalability categories, the CGS (Coarse-Grain Scalability), the MGS (Medium-Grain scalability) and the FGS (Fine-Grain Scalability).

### 3.3. The H.264 SVC encoding/decoding application

SVC In current paragraph all the above information will be modeled and implemented into Java code. The main goal is to model the H.264/AVC in a way that SVC extensions that was described above will be available. So further to previous paragraphs the use case scenarios diagram will be the below.
After these three development cycles, the final class diagram is the below.

Figure 4: H.264 Encoder/Decoder application class diagram after development cycles.

4. **Server-client application and communication protocols**

The chapter contains telecommunication protocol analysis for RTP (Real Time Protocol) and RTSP (Real Time Streaming Protocol) and their implementation in a client-server application which will use them efficiently in order to be able to transfer a real time video stream.

4.1. **The RTP (Real Time Protocol)**

Multimedia real time applications and communications demand specific QoS (Quality of Service) requirements. These requirements mostly refer to the maximum permitted packet delay, the jitter, the error rate and throughput of the communication channel. For these reasons, TCP (Transmission Control Protocol) is incapable for handling real time data as it requires retransmissions when a packet is lost and adds end to end delay to transmissions. UDP (User Datagram Protocol), which is usually employed in
such applications, does not provide any flow control mechanism and packet delivery is not guaranteed.

Consequently, RTP (Real Time Protocol) has been proposed by IETF (Internet Engineering Task Force) for end to end real time data communications. It was mainly designed for multimedia applications such as video and audio conferencing, in multicast or unicast networks. Nowadays, it is employed by the majority of streaming servers and applications. RTP is consisted of two protocols: the RTP for real time transmissions and the RTCP (RTP Control Protocol) for streaming control (EL-MARAKBY, Randa and Hutchison, David, 1996).

An RTP packet is consisted of two parts, the RTP header and the RTP payload. The RTP payload is following the RTP header and it is the actual information that the packet is carrying. The RTP header holds the information the mechanisms that the protocol provides. Below table presents the mandatory first 96 bits of the header field of an RTP packet.

<table>
<thead>
<tr>
<th>Field</th>
<th># bits</th>
<th>Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>2 bits</td>
<td>This field identifies the RTP version. Current version is 2.</td>
</tr>
<tr>
<td>Padding</td>
<td>1 bit</td>
<td>Is used mainly by encryption algorithms which add bytes until they reach a fixed size. When padding field is set to 1, means that padding bytes are added after the payload bytes.</td>
</tr>
<tr>
<td>Extension</td>
<td>1 bit</td>
<td>Identifies if a header extension is added after the mandatory RTP header bytes</td>
</tr>
<tr>
<td>CSRC count</td>
<td>4 bits</td>
<td>The count of Contributing Sources is used for combined stream by RTP mixer.</td>
</tr>
<tr>
<td>Marker</td>
<td>1 bit</td>
<td>Marker is used by a profile in order to specify significant events.</td>
</tr>
<tr>
<td>Payload Type</td>
<td>7 bits</td>
<td>Specifies the format of the payload and helps receiver to reproduce the packet efficiently.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>16 bits</td>
<td>It is an incremental number of sent packet and helps receiver to re-order packets if are not received in correct order.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>32 bits</td>
<td>It is used for synchronization and jitter calculations.</td>
</tr>
<tr>
<td>SSRC</td>
<td>32 bits</td>
<td>Source Synchronization is chosen randomly and it helps for distinguishing different RTP streams.</td>
</tr>
</tbody>
</table>

Table 2: The RTP header fields.

4.2. The RTSP (Real Time Streaming Protocol)

RTSP (Real Time Streaming Protocol) was mainly designed to manage data streams. It was not designed to carry the data stream itself but to establish controls on them.
RTSP is able to operate in both TCP and UDP. It is also possible to cooperate with RTP without having to use the same protocol. For example, RTSP could use TCP for reliable stream management while RTP could use UDP for soft real time stream transferring (SCHULZRINNE, H. et al., 1998).

RTSP support three main functions. The first one is that client can request and receive media from a server via http or other method. Another functionality is that a media server can be invited and participate in an existing real time conference. At last, protocol can indicate when a media source is available while live streaming session is ongoing. Below figure shows some typical RTSP transactions.

4.3. The server-client application

In this section a client-server application for live real time video streaming will be designed and implemented. The application that will be developed is able to run in two instances, as a server or as a client. The server should be able to capture the RTP video stream from a connected web camera and transmit it to the client. Client should be able to receive the stream and be able to represent it to a player.

For controlling the video stream, RTSP (Real Time Streaming Protocol) will be implemented using TCP. Client should be able to generate requests such as SETUP, PLAY or TEARDOWN and send them to the server. Server should be able to parse these requests and proceed with them.

For video transferring the RTP will be used on the top of UDP. Server should be able to generate RTP headers as in table 3.1 and RTP payload which contains the captured frames. The frames should be sent to client via UDP socket. Client should be able to “listen” to incoming UDP packets and analyze the header and payload bytes.

Client should be embedded in a Java Applet in order to be able to run software through browser. The main sequence of the software is presented in the next diagram.
Next two figures represent the use case scenarios diagram and the final generated application class diagram consequently.

**Figure 6:** Client-server application typical sequence.

**Figure 7:** Use case scenarios diagram for the client-server application.
5. Interface between applications and channel adaptability

This chapter describes the interface between the applications created in chapters two and three. To be more specific, the captured images will be coded using the H.264 SVC application created in chapter two and will be sent to the network using the application created in chapter three. Furthermore, the whole system will be able to adapt the bit rate and quality to the current channel conditions. For this reason RTCP (Real Time Control Protocol) will be implemented in order to provide feedback for the lost packets and make the sender adapt the bit rate and quality accordingly.

5.1. Client-server application interface with H.264 SVC

For testing purposes, the codec that was used in the server client application was the MJPEG which codes each frame independently. In this paragraph the MJPEG coding will be replaced by the H.264 SVC application developed in chapter two and unified application will be created.

For this purpose, the individual applications are considered as two different packages of the same application. The first step for this implementation is to organize frames in GOPs and initialize the SVC class. After a GOP is transmitted the SVC is re-initialized with the same or different parameter values and a new GOP is generated and is ready for transmission.
5.2. The RTCP (Real Time Control Protocol)

RTCP (Real Time Transmit Protocol) as already mentioned in chapter three is used for providing feedback about reception information and indicate the channel quality. For the current project the packet loss will be measured so that a further analysis of the loss RLE (Run Length Encoding) report blocks/packets will be provided. The RTCP transactions will be as described in the below figure.

![RTCP procedure diagram](image)

**Figure 9:** RTCP procedure diagram.

There are two classes for this implementation which are the RTCP packet class and the RTCP chunk class. For transmitting the RTCP information a TCP socket should be used and the information should be gathered there and analyzed.

5.3. Channel adaptability

In the following paragraph the RTCP will be embedded in the application. The packet and frame losses will be evaluated by the server side application and H.264 SVC will be updated accordingly. That is how the system is going to be adjusted to the channel conditions. A whole protocol system overview is displayed in the next figure.

![System protocol overview](image)

**Figure 10:** System protocol overview.
For adjusting the speed and the bandwidth utilization the server application should have some standards values and decide if the SVC could increase or decrease the transmitted bit rate. For example, if the packet loss percentage reaches a max value (“lossy” channel), then bit rate should be decreased. On the other hand if it reaches a minimum value (“healthy” channel), then bit rate should be increased.

6. Testing, results and evaluation

In previous chapters a system was designed and developed which is capable of managing web cameras and transferring real time video using H.264 SVC codec. Furthermore system is able to change the transmission bit rate according to the packet loss which is calculated by the implementation of the RTCP protocol. In this chapter, the application will be tested and evaluated under specific environments and conditions.

6.1. Testing conditions

The main nodes of the application are the “client” PC (running the client applet), the “server” PC with a connected web camera (running the server side of the application), a DSL (Digital Subscriber Line) router and an Inmarsat Fleet Broadband 250 satellite system providing speed up to 284 kbps. The main topology that will be used for testing is the below.

![Figure 11: The main system testing topology.](image)

6.2. Bandwidth utilization for satellite usage

In this paragraph the application will be tested over satellite and packet loss with bandwidth utilization will be measured and evaluated.

Tests took place in SRH Marine Electronics S.A located in Piraeus using a Sailor FBB (Fleet Broadband) 250 as described in previous paragraph. Testing the application using H.264 SVC gave some very positive results. The most positive of all was the low bandwidth utilization and that the application was always adapting smoothly to packet loss rate.
There was an expected delay of about 3-4 seconds (which is normal for such technology) but with no interruptions. The quality was satisfying even though the packet loss rate was about 33-34% at most of the times. In the next figure an output of the server side application is presented for RTCP protocol adaptation. The RTCP was configured to speed up when loss is less than 5% and slow down when loss rate is greater than 10%. That is why the application was transmitting at the minimum bit rate at most of the times.

![Figure 12: Application RTP utilization over satellite](image1)

![Figure 13: Application server side output screenshot for RTCP](image2)

The RTP average bandwidth utilization is about 6.7 kbps. Also from above figure is clear how the bit rate is reduced during transmission. It started from a nearly maximum bit rate transmission of about 30 kbps and reached very low values of about 6 kbps. The RTCP and RTSP bandwidth utilization overhead has also been monitored and it is presented in the next figure.

![Figure 14: Application utilization of RTCP and RTSP](image3)

The average overhead utilization of RTCP and RTSP protocol is about 0.05 kbps. The first peak of the graph is for RTSP negotiation and the periodical peaks are due to the RTCP packets. The fact that the RTCP time gaps are not steady is because the SVC is adjusting the frame rate. Below is an overall bandwidth utilization for RTP, RTSP and RTCP protocols.
In the next figure a screenshot of the application during testing over satellite in SRH Marine premises is presented.

Figure 16: Application screenshot during testing over satellite.

6.3. Quality evaluation

For objective quality evaluation PSNR was calculated locally for MJPEG compression and H.264 xuggler compression. Results showed that MJPEG seems to perform better than H.264 implementation of xuggler library.

For subjective quality evaluation ten people were presented four different videos. Results are presented in below table.

<table>
<thead>
<tr>
<th>Tester</th>
<th>MJPEG (LAN)</th>
<th>MJPEG (Sat)</th>
<th>SVC (LAN)</th>
<th>SVC (Sat)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tester 1</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Tester 2</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Tester 3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Tester 4</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Tester 5</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Tester 6</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Tester 7</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Tester 8</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Tester 9</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Tester 10</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Results show that SVC operates better than MJPEG over satellite. The main reason for this is that the bigger image packets of the MJPEG lead to high packet loss and many video interruptions have been monitored. Another reason is that the bit rate of MJPEG was stable, and when the available bandwidth was reduced the system was not able to adapt to it.

7. Conclusions

Satellite systems are able to provide worldwide coverage but communication channel are suffering from weather effects, network delay, jitter effect, high average of packet loss and low available bandwidth.

For achieving a system that will be able to transfer video stream efficiently, the coding standard, session control and error control are the main issues that should be considered. Especially H.264 SVC can provide bit rate scalability and seems appropriate for satellite usage. Furthermore RTP, RTCP and RTSP can add efficiency to video transferring by also adding error and session control.

Testing the application in satellite environment, gave back some positive results in a channel where an average of 33-34 % packet loss was reported by RTCP. System was able to reduce the bit rate and transfer video efficiently. Subjective quality evaluation showed that MJPEG performs better than xuggler library for H.264. Objective quality evaluation showed that MJPEG can perform better when bandwidth is enough, while H.264 SVC can perform better in low and unstable bit rate environments when application is able to adapt to it.

References

Appendices

Appendix I: Prototype system class diagram overview.

Name: _____________________________________
Surname: ____________________________________________
Age: ______
Education: High School / TEI / University / Post graduated / PhD
Business Profile: ________________________________________________

<table>
<thead>
<tr>
<th>Video 1</th>
<th>Video 2</th>
<th>Video 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢 Excellent</td>
<td>🟢 Excellent</td>
<td>🟢 Excellent</td>
</tr>
<tr>
<td>▶ Good</td>
<td>▶ Good</td>
<td>▶ Good</td>
</tr>
<tr>
<td>▫ Fair</td>
<td>▫ Fair</td>
<td>▫ Fair</td>
</tr>
<tr>
<td>□ Poor</td>
<td>□ Poor</td>
<td>□ Poor</td>
</tr>
<tr>
<td>□ Bad</td>
<td>□ Bad</td>
<td>□ Bad</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Video 4</th>
<th>Video 5</th>
<th>Video 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Excellent</td>
<td>□ Excellent</td>
<td>□ Excellent</td>
</tr>
<tr>
<td>□ Good</td>
<td>□ Good</td>
<td>□ Good</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>Fair</td>
<td>Fair</td>
<td>Fair</td>
</tr>
<tr>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
</tr>
<tr>
<td>Bad</td>
<td>Bad</td>
<td>Bad</td>
</tr>
</tbody>
</table>

**Appendix II:** Video quality evaluation form.
Development and Evaluation of Extreme scale Computing Applications

A. Lekkos¹, D. Adamopoulos²

¹ Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: a_lekkos@hotmail.com
² Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: dxa@otenet.gr

Abstract

In this paper, matters of development and evaluation in extreme scale computing systems are discussed. Various parameters - in particular system architectures, operating system noise, synchronization and speed, energy efficiency and consumption, resilience, scalability - that have to be considered when developing and evaluating extreme scale computing applications are analyzed. Also many tools (such as the ExM project, the Cielo project, the xSim project) that are frequently used in the development and evaluation of such applications are presented and then compared, discussed and analyzed. Finally, in addition to all the previous matters, future challenges on technologies related to extreme scale computing applications and systems are discussed.

1. Introduction

Everything in life is about evolution – pretty much everything around us is evolving. Since evolution has the meaning of change, nothing stays static - same as for computing systems that are the main subject of this thesis. In the very beginning of computing history, there were computer systems that were using single processors in order to function and to perform. Later on – in the mid 60’s specifically – fields like science and engineering demanded faster, larger and most of all more accurate computing performance. This demand for more power and greater complexity of computing systems led to new technologies such as supercomputing (or high performance computing as it is alternatively mentioned in many cases).

The main subject of this paper is related to extreme scale computing and furthermore, many matters and aspects of development and evaluation of applications that are commonly used in such computational environments will be discussed. In order to have those matters discussed thoroughly, before the start of this discussion it is essential to define some terms that are describing them to set the base for further analysis.

2. Development of ESC applications

In this paper development of extreme scale computing applications in extreme scale computing environments will be discussed. Much emphasis is given to the parameters that have to be considered by the developer in order to build an application that will serve in the best way possible the purposes that is meant to support. Although each
application has a unique purpose and use, there are common parameters in application development that define the criteria that every application must meet. These parameters are going to be discussed and analyzed later on by this thesis, one by one and in a way of descending importance.

3. **Evaluation of ESC applications**

Evaluation is a way of testing some aspects of an application that is developed or is to be developed, as we will see later on. The standards that are used and the parameters that are considered during the process of evaluation are discussed and presented. Evaluation is an important procedure that can reveal the weak points of an application, the parts that need improvements and on the other hand the strong points and the part that hold the power of the whole application. Furthermore, with evaluation there can be comparison between two or more applications and the researchers can come to important conclusions for further methods of application development.

4. **Uses of ESC applications**

Extreme scale computing applications are commonly used in the field of science for research and development purposes, where there are computations of a high level that have to be done. An example for scientific use could be medicine or pharmaceutical design.

Apart from the scientific computing use, they can also have military use for example aeronautics and many military defense systems use extreme scale computing solutions. Furthermore, some of the fields were extreme scale computing applications are used can be of a more technological nature and may include civil engineering, electrical and electronic engineering, economic / financial analysis or even energy applications as well, where the demand for extreme performance in the computing systems that are used is of a high level (Seelam et al., 2013).

Extreme scale computing also involves in databases and in services that concern cloud computing and storage – a field that uses such services is economics, web service providers and others. Among the largest corporations that use extreme scale computing technology in their servers, platforms, means of storage and databases in order to provide high level and performance services to their customers and users, are Google and Yahoo. First there was Google with the launching in early 2007 of a distributed storage system under the name Bigtable (Chang et al., 2008) and then Yahoo followed later on. Researchers for Yahoo described in 2008 and then launched in 2009 a hosted data serving platform under the name PNUTS (Cooper et al., 2008).

As a general conclusion, it has to be mentioned at this point that extreme scale computing helped increasing by far the computational capabilities of the systems that are used in the previously mentioned human activity fields meeting the needs of computational science for top level performance.
5. Architecture of ESC systems and applications

As it was mentioned, extreme scale computing architecture is the one that combines a series of processors in a parallel way. In the figure below, various types of architectures are presented in accordance to their popularity throughout the years (Sterling, 2012)

![Figure 2. System architectures](image)

It is the most effective architecture in high performance computing systems, due to the fact that it consumes little energy and thus provides maximum performance with considerably little cost. Apart from considering the operational cost of computing systems that use extreme scale architectures, one of the hardest tasks when building an extreme scale computing system or developing applications for such systems is combining reliability in applications with the ability of reaching high levels of performance. This combination is heavily bounded with the architecture that the computing system will be build upon. So, it can easily understood that hardware and software matters in extreme scale computing applications are not two separate fields of computing science but two fields that are depending on each other.

6. Operating system noise in ESC systems and applications

As it was previously mentioned, extreme scale computing systems are consisting of many processors that work combined together. This practically means that they work...
under specific time schedules. The main principal of this is synchronicity and it is a vital characteristic in every extreme scale computing system as it affects the way that the systems reacts and in the end, its whole function. All the protocols used, the nodes that the systems has, inputs and outputs, all the functions that are performed and even the packages delivered or send should be under the same timing, working in a synchronous manner. In cases that synchronicity is lost (this may refer to a part of the system or even to the whole system - in the worst case scenario) we have a condition which is described as operating system noise. In that case, there is failure in following the time schedules that concern all the functions of the system and the operating system noise that appears can and may cause serious problems that affect in many ways the whole system’s efficiency.

It is almost impossible that an extreme scale computing system platform can have zero operating noise, so the main concern of every measure taken is to eliminate it to the lowest possible level. The amount of noise in an extreme scale computing system is also a way of evaluating it and also a factor that has to be considered when developing applications in such systems.

A study relative with precautions and measures that can be taken in order to limit noise in operating systems comes from Beckman, Iskra, Yoshii, Coghlan, and Nataraj (2008). Due to the fact that operating system noise is caused by lack of following certain time schedules, the real issue to be addressed is synchronicity in computer systems that use large numbers of processors – and this is the main goal in the specific study. Furthermore, since high levels of operating noise can lead to interruption of applications in the system, the measures that are discussed in the following lines should be considered when developing applications that run on extreme scale computing platforms and also when evaluating them, since the presence of operating noise can be related and affects in many ways the performance of the applications that run on the specific platform.

7. Synchronization and Speed issues in ESC applications

In the vast majority of extreme scale computing systems a large number of nodes can be found and their presence has a role in the speed that characterizes the execution of the applications that are used by the system. This is a cause of reduced speed in applications that run on the system, since there is lots of synchronization to be done. This synchronization refers to data that has to be exchanged between the nodes that the system holds – the larger is the number of the nodes that a system has, the more is the amount of data that has to be transferred between them. Data flow from one node to another should be not only fast but also accurate as well. Speed and accuracy is a combination that is hard to accomplish. Due to the fact that the amount of data that is transferred in extreme scale computing systems is large and also to the fact that the number of nodes from and to which the data is transferred is large as well, the possibility of data flow errors along with lags in data transmission increases dramatically.
8. **Energy efficiency and consumption in ESC applications**

A matter that is of a highest importance when developing or evaluating an application in extreme scale computing is the consumption of energy that characterizes the application. Economy is important due to the fact that when the operational cost of a system is high, this is a suspending factor for its development - so any waste on energy matters is extremely undesirable. So application development or evaluation in extreme scale computing is based on the less energy consumption or alternatively the highest energy saving the possible. Many studies have been made on matters of energy consumption and efficiency and until now it is still an open research field with a lot of challenges for the near future, as we will see later on.

A table presenting the energy efficiency of several super computing systems according to their type and the number of GigaFLOPS that are used in it follows (Rajovic, Vilanova, Villavieja, Puzovic, & Ramirez, 2013).

<table>
<thead>
<tr>
<th>Supercomputing system</th>
<th>Type</th>
<th>GFLOPS/W</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue Gene/Q Cluster</td>
<td>Homogeneous</td>
<td>2.1</td>
</tr>
<tr>
<td>Intel Cluster</td>
<td>Intel MIC accelerator</td>
<td>1.38</td>
</tr>
<tr>
<td>Degima Cluster</td>
<td>ATI GPU accelerator</td>
<td>1.37</td>
</tr>
<tr>
<td>Bullx B505</td>
<td>NVIDIA GPU accelerator</td>
<td>1.27</td>
</tr>
<tr>
<td>iDataPlex DX360M4</td>
<td>Homogeneous</td>
<td>0.93</td>
</tr>
</tbody>
</table>

**Figure 3.** Power efficiency

9. **Addressing resilience in ESC**

According to research done by Daly and John T. (2007), failures in extreme scale computing systems often appear with the form of interruptions in applications or in less serious situations, there are applications that are running in a mode that is degraded and that is going to be discussed in the following lines, since it is a major problem that has to be considered when developing of evaluating extreme scale computing applications. These interruptions mentioned can have an impact on the extreme scale computing systems and their applications that can be divided in two large categories.

10. **Scalability of ESC systems and applications**

The most successful system architectures in extreme scale computing are those who are able to deal with scalability limitations. A high performance computing system should be able to welcome any adjustments made to its architecture and specifically the adding of more processors and the enlargement in the topology of the whole system in general. In computational science, this ability to adjust to changes like the ones that were above - mentioned, is generally referred as scalability of the system. Scalability may refer to the hardware of the system or to its software and applications.
Important tools in development and evaluation of ESC applications

11. The Extreme – scale Many – task (ExM) project

Armstrong et al. (2012) in the University of Chicago, the University of Columbia and Argonne Leadership Computing Facility at Argonne National Laboratory produced an advanced hierarchical model that can be used not only for programming but also for executing applications in extreme scale computing systems. Its name was ExM (after the initials Extreme – scale Many - task) and although it was originally designed to be applied on petascale computing systems, all of its structure and all the functions that it can perform can be easily updated and adjusted in exascale computing systems as well. Of course ExM can fully support almost effortlessly computer systems that are build on smaller scales - such as for example gigascale of terascale systems – but in this paper we will focus on modern technologies – such as petascale and exascale systems that are the dominant part of computational science field nowadays. Since scalability in extreme scale computing is of a high importance, ExM with his high adaptability in larger scale systems is very promising for the future of computational science. In addition to the above, ExM project is also capable of evaluating extreme scale computing applications. Applications in ExM consist of a number of computational tasks that are combined together and work in a synchronous manner. Supporting of those tasks not only in terms of execution but also in generation terms, this project uses a script language named Swift. Swift language is the one that manages issues related to the tasks (mainly those two that we have mentioned) that are performed by the system and it is responsible for the smooth operation of the whole system in general. Application development with ExM follows an alternative way from the one that is usually followed in application development methods and styles – it addresses tasks as an external part of the computing system and each application is developed as a library out of the system or in some other cases as an executable program that is linked to the system externally. It also offers hierarchical distribution on data flow issues, which can be energy – friendly without sacrificing much from the resilience that the system must have.

12. Cielo project

A very interesting piece of work comes from Vaughan et al. (2010) and was developed in Los Alamos and Sandia National Laboratories, located in New Mexico. There, in the year 2010, a high – level requirement petascale computing system was developed in replacement of a high performance computing system that was used in the Lawrence Livermore National Laboratory.

The name of the project was Cielo and it was developed for appliance on national security defense systems, an area which - as it was previously mentioned - uses frequently extreme scale computing technologies. Cielo’s main purpose as a project was to perform complex calculations in both nuclear and non – nuclear weapons by means of modeling in the very beginning, simulating afterwards and finally measuring and validating the performance of the weapon systems and in general the processes that are followed during the use of such systems by the U.S. Army. Workload had the form of packets. The traffic was determined by a number of factors based on the
importance and the worthiness of each packet that were setting priorities and controls over packet traffic. All data concerning the simulations and modeling provided by Cielo offered great help on fields of research, development and also experimentation on nuclear and non–nuclear weapon systems that were used by the National Defense Forces.

13. The Extreme - scale Simulator (xSim)

Christian Engelmann along with Thomas Naughton working at Oak Ridge National Laboratory (Engelmann & Naughton, 2013) developed a toolkit under the name xSim) or Extreme – scale Simulator as it is its full name). During the development of xSim, Engelmann and Naughton focused on three specific fields of computational science. The first one was matters of performance that was related to extreme scale computing systems, the second one was resilience in those systems (that is relevant to performance and was analyzed above) and finally the third one was the hardware and software power consumption in relation to the architecture that is chosen for an extreme scale computing system. In the third field, the cost of building a system with a specific architecture (various types of architectures are examined) is taken into consideration and is related with the performance and resilience that can be offered by the specific system that is investigated – this cost can be inserted as a parameter in the xSim toolkit and after the toolkit process this data, relevant to it results can be obtained. In order to examine power consumption issues, power consumption models were built and tested on different parts of various extreme scale computing systems, measuring and monitoring the voltage, the frequencies and the amount of energy that was spent during the system’s operation. In many cases, injection of faults in the systems was also used as a technique, to examine the overall fault tolerance of the system and its applications. It is very important to be mentioned at this point that xSim toolkit can also support fault injection to the system that is examined by it. This is one of many radical characteristics that this specific toolkit holds, along with its unique ability to be maintained and optimized by inserting data that concern system’s desired resilience and desired performance of the system’s applications as well. The research and the xSim toolkit that was produced out of it focused mainly on applications that were related with proxies, on applications with the ability to offer fault tolerance to the platforms of the systems that they are running and finally on creating benchmarks that would be used as standards set for future benchmarking tests that will be applied on extreme sale computing applications and systems. The xSim was one the most influential developments on the extreme scale computing during the last few years and that was shown also in the amount of discussion that followed after the day that it was presented to the scientific community and the public.

14. Conclusions

Many different methods and techniques are developed are numerous other are soon to be developed on applications that are used in extreme scale computing systems in the near future. In this paper there was a brief presentation of the some of the most important of them, while others having not so great importance and rank, were
presented with less detail as they are less efficient or offer fewer and minor advantages than the others.

Scalability is one of the key factors in extreme scale computing application development and evaluation, because applications and systems should be able to adjust to higher scales and perform without faults or interruption but with efficiency and accuracy, in order to follow technological advance and to stay up to date with the current and future technology. So we could say that scalability offers an open door to future of extreme scale computing applications and systems and the progress that is taking place in this field of computational science.

Right next to scalability lies resilience, an also important feature that must be considered when developing or evaluating applications, since they have to be reliable, available and maintainable as well. A field that availability has crucial importance is in medical and energy applications, where lack of it may have cost even in human lives. The key to resilience is the monitoring of the system and its applications, in order to prevent or deal in an efficient way with any matter that is related to reliability, availability and maintenance of the system and all of its applications.

A number of tools providing all of these previously – mentioned factors was presented and compared with the most important ones to have the highest number of advantages, like the ExM or the xSim projects and others to be focused on specific subjects. As a general conclusion, extreme scale computing applications are the most vital part in high performance computing and their evolution is a very important field of the computational science. Their uses offer a lot in fields of human activity that have crucial importance. Their development and evaluation lies heavily on the factors that were analyzed (such as architecture, resilience, scalability, energy efficiency and consumption and so on) and can be assisted by tools that were presented in this thesis (such as Cielo, ExM, xSim).

References


Network Bandwidth Estimation

Dimitrios Mantzioris\textsuperscript{1}, A. Papadakis\textsuperscript{2}

\textsuperscript{1} Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: dmantzioris@hotmail.com

\textsuperscript{2} Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: andreas.papadakis@gmail.com

Abstract

Estimating available bandwidth accurately is extremely important for many network related applications, especially the ones which need real-time traffic information. With the ever-increasing use of Internet, several available bandwidth measurement techniques have been proposed. Specifically, this thesis examines the available algorithms for precise Available BW measurement. The majority of such available algorithms measure the available BW using techniques such as active-probing and client-server tools. Algorithms have been developed using mathematical models each with their inherent assumptions. In some cases the variation of the available tools can be beneficial to the user while in other cases it may prove to be a challenge. It provides detailed description of the structure and characteristics as well as the installation methods of the networks case study. The experimental results are presented along with the analysis of the measurements acquired by the various tools used in the installed networks. The results are validated using application layer tools. Conclusions are drawn from the acquired results and are evaluated based on the usefulness and the ease of use of the respective tools utilized during the experimental procedure.

1. Introduction

The recent unprecedented development of the area of network technology has sparked a constant demand for reliable network service provision in various types of networks. A variety of tools was developed and implemented to monitor the behaviour and characteristics of each type of network. The network characteristics of concern are the link capacity, available bandwidth, transmission delay, transmission loss and network topology\textsuperscript{[1],[2]}. The monitoring results can be directly applied in the management and maintenance of the computer networks as well as on the troubleshooting of existing conditions. There are numerous on-line applications that base their operation on the calculation of available bandwidth. Calculating the available bandwidth of an end-to-end network path can significantly impact the quality of the service itself. In order to optimize their performance, such applications typically require real time network information. Therefore the available BW of each path impacts the network performance. This results to maximum transmission rate of data along a path, without the interference of the transported cross traffic. In addition, knowledge of the end-to-end available BW is used during the flow control process, which in turn prevents network congestion. Finally, network engineers can use the available BW to reroute data traffic as well as in the design of future network expansions.
During the last 15 years a large global research effort was undertaken in order to develop methods of reliable measurement of available BW. Precise measurement of available BW is a rather painstaking and challenging effort as it is impacted by fluctuating and discrete parameters. The main parameters that interfere with the precision of BW measurement are the location of bottleneck link, the tight linking of the path and the path’s cross-traffic rate. Other parameters of concern during BW measurement include network complexity, network topology and transfer models, as well as the possibility of the measuring packages declining from the Intrusion Detection Systems (IDS).

The majority of such available algorithms measure the available BW using techniques such as active-probing and client-server tools.[3],[4] Algorithms have been developed using mathematical models each with their inherent assumptions. In some cases the variation of the available tools can be beneficial to the user, while in other cases it may prove to be a challenge. For example, a tool may be ideal for the investigation of a high speed rather than a slow speed connection. A part of this paper provides a short description of the structure, and characteristics as well as the installation methods of the networks case study. The structures presented in this study are used as test methods of the tools used to measure the available BW. The experimental results are presented in part 4 along with the analysis of the measurements acquired by the various tools used in the installed networks. In part 5 the results are analyzed using application layer tools. Conclusions are drawn from the acquired results and are evaluated based on the usefulness and the ease of use of the respective tools utilized during the experimental procedure.

2. A Survey of Tools

1.1. Passive and Active Measurements

The measurement of network characteristics can be divided in to two major categories. The method used is based on either a Passive or an Active measuring technique. Passive measurement is a method of monitoring the efficiency and behaviour, as well as traffic of the data packages without creating new ones or modifying the traffic. Passive measurements can be implemented using the network’s routing devices, and by noting the characteristics and quantity of packages going through. This method allows us to draw certain statistical parameters that describe the network without inserting any additional packages in the system. The nature of the flowing packages as well as the level of our analysis will determine the accuracy level of the collected data. On the downside, this method requires equipment which accesses security issues we need to own and if we do not own the network we are not allowed to tap our devices in it. [3]

A separate approach of measurement is that of active measurement. This method requires the insertion of additional data packages in the system. These additional packages assist the active measurement. One of the advantages of this method is that it does not require complete security access to the network. Unavoidably, this method places additional traffic to the system by introducing an additional package load, which the system needs to handle. [3]
1.2. Client – Server and Standalone Measurement Techniques

The measuring tools of the available BW fall under two main categories, the client-server and the standalone. The tools based on a client-server interface must be installed in the source host and the destination host, which monitors the flow and records the corresponding measurements. On the other hand the standalone tools must be installed only in the source-host terminal. The difference of this specific technique is that the two way active technique performs measurements in both directions of the path. Client-server tools are composed of various softwares which are installed in the two communicating terminals. During the measurement process the sender sends packet trains in various rates. On the other hand the packets arrive at the receiver time-stamped. Typically it is very difficult to accomplish a measurement without collaboration - access to the destination host. A common challenge typically encountered by the users of client-server tools is that, although they can install the tool in the local terminal, they cannot install it in the remote location, since they do not have direct access to it. Later we shall demonstrate how a user can overcome such a challenge.[4]

Unlike client-server tools stand-alone tools only need only to be installed in the sender-host. The method of operation is based on an algorithm that sends a series of data packages (ICMP echo - request) using the timestamp of the incoming packages to perform the measurement. The downside of this tool is the limited or restricted access of the sender-host to the receiver host computer. There are plenty of web locations which can determine the quality of the provided service, after they have performed the network quality measurement.

1.3. Tool categories

Gap-based and rate-based tools are the two types of tools currently available for this technology, but because of the variety of approaches each one uses to conduct measurements as well as the underlining models on which they are based they can easily be considered six separate models. These categories are gap - based, rate - based, model - based, probabilistic, hybrid and Kalman filtering based.

The Gap-based tools are usually materialized by packet pair / train data. The export of data utilizes information of the time gap between two successive arrivals of data, which are detected successfully by the receiving end. The advantage of this method is the sensitivity to the burstiness of cross - traffic because of the fine gained interaction between probing data packages and data packages of cross -traffic. The process scheme shown in figure 2.1 illustrates the gap-based approach. [5]
Most researchers prefer the rate-based approach to measure the available BW in a path. Such a technique is based on the congestion that exists in the path due to the tool itself. For example, if someone is sending probe traffic at a smaller rate than the path's available BW then the rate of probe traffic that reaches the receiver is the same as the one initially sent by the sender. On the contrary, if the probe traffic is sent at a greater rate than the available BW, then queues will form in the network and there will be delays in the probe traffic transference. As a result, the probe's transfer rate will be slower than the one initially sent by the sender. The measurement of the available BW can be found when the probe traffic of the receiver and sender are equal.\[5\]

The model based approach is a category of tools that was developed based on the model-constructing of the network traffic. They perform best when both the network structure and the cross-traffic follow the same assumptions as the ones used during the development of the tool. One of the disadvantages is that their performance drops when the network or mode of transfer where the measurements will take place diverge from the model of the original network on which they were initially developed. \[6\]

Besides the previously mentioned measuring methods of available BW a probabilistic analysis approach can also be utilized. There are two statistical tools available the SMART and the A_ABE. The main purpose of these tools is to measure accurately the available BW where most gap-based approach tools fail. \[7\]

The Hybrid measuring of the Available BW tools aim to combine the gap-based and rate-based approaches. That is accomplished using train structures of existing algorithms while attempting to incorporate all the advantages of both approaches in a single tool. In order to understand the modus operandi of the hybrid approach it is of the greatest interest to provide an example. Gap-Based algorithms require a known bottleneck capacity of the path but they are less intrusive than rate-based algorithms. On the other hand, rate-based algorithms do not require any previous information about the network, but they send a great number of probe packets, typically causing network congestion. \[8\]

The Kalman filtering based algorithm is a category of approach of available BW measurement which is based on the Kalman Filter. The Kalman filter is a widely accepted and user friendly filter which allows us to get rid of faulty measurements. This algorithm conducts a theoretical estimation of the network values and then uses the measurements in order to correct the initial estimation. Therefore it has the capability of
providing estimates with a smaller margin for error than the one of the measurement. It is an expansion of the Least Squares methods, which is a group of mathematical equations that introduces the estimation-correction scheme, the most efficient in terms of minimizing the error variability when the network setup and the measuring "noise" have been modelled accurately.[9],[10]

3. Experimental environment

The experiments were implemented in four different network structures. These network structures are named in a descriptive way as i. LAN test bed 10/100 Mbps, ii. LAN test bed wireless 54 Mbps, iii. xDSL to xDSL test bed via VPN and iv. xDSL to 3G test bed via VPN. The four network structures are presented shortly in this chapter. As is well known, the majority of tools performing such measurements have been implemented in programming language C++. Therefore it is considered necessary to use an operating system that can do compile and 'runs' such tools without reducing the network capabilities. The operating system used in all the terminals of the experiments is the Ubuntu 13.1.

3.1. How and why to setup a VPN network

As long as measurements are carried out on internal LAN tools, things are networked 'easily'. But when the measurements are performed in network environments where there is no management, then this 'easily' turns into a difficulty which increases exponentially. The overwhelming majority of the tools perform measurements via communication from specific ports. A solution could be to port forward certain ports of modem / routers and the related settings of the experiment terminals whenever there is experiment. However this is considered technically unprofitable because ISPs have policies that limit the available services and because it is time consuming to adjust our networks every time that we change a tool. The solution to this problem is to install VPN connections via internet on experiment terminals. This is achieved by using software
which creates the VPN connections using virtual ethernet cards. In this way there are terminal connections located on the internet with the ease of management that a LAN network offers. [11]

3.2. Experiments conditions - configuration

This section refers to the conditions of the experiments and to the way the tools are configured. Throughout the course of the measurements to the networks of experiments there was only traffic that originated from network cards of terminals, which were, in some way, in idle mode. To be more specific, during the operation of the network tools there were only data packets corresponding to the tool being tested at that time. Knowing this fact, we could say that the available BW is identical to the BW. However in measurements of telecommunications networks there are affecting factors which make the engineer's job more difficult. In this case we have secured the network adapters through blocking the other ports that will not be diverted to additional network data packets from network cards of test terminals. It is also necessary to mention that the communication with the remote terminal was achieved by using RDP connection which was interrupted immediately after starting the tool, without affecting taking measurements of the available BW. The RDP connections were used only in xDSL to xDSL and xDSL cases to 3G network measurements. In tables of appendix 1 to 7 there are the settings of the tools during the execution of the experiments.

4. Analysis

4.1. Measurements of tools

This chapter presents the experimental results and the statistical analysis preformed on the measurements acquired by the tools of concern. It is of great importance to capture the measurement reliability provided by all tools. Figures 4.1 through 4.4 show the graphical depiction of the measurements acquired by the respective tools used in the various networks. A number of the tools tested did not yield results when used to measure in specific networks.
4.2. Relative error of tested tools

This unit presents the tables or relative errors of the tools tested in the various network configurations. It must be noted that the tables 8 to 11 (see appendix) demonstrate the relative errors of measuring tools, as they were used in the various networks, which is analogous to the statistical reliability of the measurements. This statistical analysis yields important conclusions about the respective tools used.

After careful consideration of the statistical results of the tools implemented it can be noted that on Lan test bed at 10/100Mbps all the tools yielded small relative errors, irregardless of the number of measurements. Only two of the eight tools tested yielded a relative error greater than 5%. In the network configuration Lan test bed wireless 54Mbps the relative error remains low, and therefore the results are reliable as well, having only two tools with a relative error of greater than 5%. The reliability decreases, due to an error increase in between 5% and 10% in the case of the topology xDSL to xDSL via VPN. In this case only two tools yielded errors less than 5% Finally in the topology of xDSL the 3G via VPN three out of eight tools did not yield any results while one tool yielded only a single measurement. Out of the four remaining tools, three
show an error of measurement greater than 5% and one shows an error of measurement of less than 5%.

5. Comparison of tools

The majority of tools presented perform physical layer measurements. Iperf, on the other hand, measures the available BW at an application layer level. Iperf also conducts measurements for the entire data set between end - hosts during the transport period. It is important to note that transport layer was designed in such a way so as to allow equal-sized node entities to maintain communication similar in level with that of model OSI.

In this unit we will compare the results maintained by the tools tested in all the experimental networks, as a function of the reliability of each tool presented in analysis part. It cannot be omitted that the error shown in the figures presented in analysis part represents the agreement which concerns the criterion of the error of measurement. In this current analysis this criterion was utilized under a normally distributed set of measurements. Table 12 of appendix allows for an easier comparison of the graphical representation of the data, where a summary of all the Relative Errors are presented. This summary includes the errors measured while using Ubiquiti Networks and NetStress tools. Figures 10-13 show a representation of the cumulative results of the tools tested in the four specific network topologies. The blue dot represents the average measurement. The lines extend to show the range off all the measurements provided by the tools.

![Figure 10](image1.png) ![Figure 11](image2.png)

**Figure 10**: Interval Plot of tested tools on LAN test bed 10/100 Mbps.
**Figure 11**: Interval Plot of tested tools on LAN test bed wireless 54 Mbps.
6. Conclusion

This paper demonstrates a comparison of various tools and their respective approach techniques in an effort to determine the available BW parameter. The implemented approximation techniques of the various tools provided a great insight and also exposed their inherent weaknesses. In order to assess the reliability of the measurements, the experimental data could be fit into various distributions other than the Normal, but for this assessment the normal distribution was consciously selected as the most appropriate. The number of measurements could have been greater, yet that would impose a great time burden to the study and the results’ reliability would not necessarily improve. It is important to note that the reliability of measurement dropped significantly when moving from the Lan and Wireless Lan to xDSL to xDSL and xDSL to 3G. The greatest drop of reliability was noted when moving from a xDSL to 3G test bed, in which the majority of the tools tested did not yield any results.

Two out of the four network topologies in which the tools were tested yielded similar results, while the other two yielded greatly deviating results. This deviation rendered necessary a validation of the tools using a software that conducts measurements at a higher level network than the one in which the tools tested typically operate. Iperf offered the greatest measurement validation available in the xDSL to xDSL and xDSL to 3G network topologies. Iperf enabled us to determine the real achievable available BW of these networks. Matching the values yielded by Iperf was an indication of a tool’s reliability.

Further research effort could be geared to a more detailed evaluation of a smaller number of tools or even a single tool. A great amount of insight could be harvested by the investigation of a single tool which would be tested in varying network configurations.

References

Appendix

**Table 1: DietTopp Configuration.**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lan test bed 10/100 Mbps</td>
<td></td>
</tr>
<tr>
<td>Lan test bed wireless 54 Mbps</td>
<td></td>
</tr>
<tr>
<td>xDSL to xDSL test bed via VPN</td>
<td></td>
</tr>
<tr>
<td>xDSL to 3G test bed via VPN</td>
<td></td>
</tr>
<tr>
<td>It is not available to change configuration.</td>
<td></td>
</tr>
<tr>
<td>It is not available to change configuration.</td>
<td></td>
</tr>
<tr>
<td>It is not available to change configuration.</td>
<td></td>
</tr>
<tr>
<td>It is not available to change configuration.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 2: Pathload Configuration.**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lan test bed 10/100 Mbps</td>
<td></td>
</tr>
<tr>
<td>Lan test bed wireless 54 Mbps</td>
<td></td>
</tr>
<tr>
<td>xDSL to xDSL test bed via VPN</td>
<td></td>
</tr>
<tr>
<td>xDSL to 3G test bed via VPN</td>
<td></td>
</tr>
<tr>
<td>By default configuration</td>
<td></td>
</tr>
<tr>
<td>By default configuration</td>
<td></td>
</tr>
<tr>
<td>By default configuration</td>
<td></td>
</tr>
<tr>
<td>By default configuration</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3: Iperf Configuration.**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lan test bed 10/100 Mbps</td>
<td></td>
</tr>
<tr>
<td>Lan test bed wireless 54 Mbps</td>
<td></td>
</tr>
<tr>
<td>xDSL to xDSL test bed via VPN</td>
<td></td>
</tr>
<tr>
<td>xDSL to 3G test bed via VPN</td>
<td></td>
</tr>
<tr>
<td>The length of buffers to read or write, (-l)</td>
<td>8 KB</td>
</tr>
<tr>
<td>The length of buffers to read or write, (-l)</td>
<td>8 KB</td>
</tr>
<tr>
<td>The length of buffers to read or write, (-l)</td>
<td>8 KB</td>
</tr>
<tr>
<td>The length of buffers to read or write, (-l)</td>
<td>8 KB</td>
</tr>
<tr>
<td>Other adjustments by default</td>
<td>Other adjustments by default</td>
</tr>
<tr>
<td>Other adjustments by default</td>
<td>Other adjustments by default</td>
</tr>
<tr>
<td>Other adjustments by default</td>
<td>Other adjustments by default</td>
</tr>
</tbody>
</table>

**Table 4: PTR-IGI Configuration.**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lan test bed 10/100 Mbps</td>
<td></td>
</tr>
<tr>
<td>Lan test bed wireless 54 Mbps</td>
<td></td>
</tr>
<tr>
<td>xDSL to xDSL test bed via VPN</td>
<td></td>
</tr>
<tr>
<td>xDSL to 3G test bed via VPN</td>
<td></td>
</tr>
<tr>
<td>The number of train probed for each source gap, (-N)</td>
<td>3</td>
</tr>
<tr>
<td>The number of train probed for each source gap, (-N)</td>
<td>3</td>
</tr>
<tr>
<td>The number of train probed for each source gap, (-N)</td>
<td>3</td>
</tr>
<tr>
<td>The number of train probed for each source gap, (-N)</td>
<td>3</td>
</tr>
<tr>
<td>The number of probing packets in each train, (-n)</td>
<td>60</td>
</tr>
<tr>
<td>The number of probing packets in each train, (-n)</td>
<td>60</td>
</tr>
<tr>
<td>The number of probing packets in each train, (-n)</td>
<td>60</td>
</tr>
<tr>
<td>The number of probing packets in each train, (-n)</td>
<td>60</td>
</tr>
<tr>
<td>The length of the probing packets in bytes, (-s)</td>
<td>1024</td>
</tr>
<tr>
<td>The length of the probing packets in bytes, (-s)</td>
<td>1024</td>
</tr>
<tr>
<td>The length of the probing packets in bytes, (-s)</td>
<td>1024</td>
</tr>
<tr>
<td>The length of the probing packets in bytes, (-s)</td>
<td>1024</td>
</tr>
<tr>
<td>Other adjustments by default</td>
<td>Other adjustments by default</td>
</tr>
<tr>
<td>Other adjustments by default</td>
<td>Other adjustments by default</td>
</tr>
<tr>
<td>Other adjustments by default</td>
<td>Other adjustments by default</td>
</tr>
<tr>
<td>Other adjustments by default</td>
<td>Other adjustments by default</td>
</tr>
</tbody>
</table>
### Table 4: PTR-IGI Configuration.

<table>
<thead>
<tr>
<th>Pathchirp</th>
<th>Lan test bed 10/100 Mbps</th>
<th>Lan test bed wireless 54 Mbps</th>
<th>xDSL to xDSL test bed via VPN</th>
<th>xDSL to 3G test bed via VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Parameter</td>
<td>Value</td>
<td>Parameter</td>
</tr>
<tr>
<td>The experiment duration (secs) (-t)</td>
<td>200</td>
<td>The experiment duration (secs) (-t)</td>
<td>200</td>
<td>The highest rate (Mbps) to probe at within chirp (-u)</td>
</tr>
<tr>
<td>The lowest rate (Mbps) to probe at within chirp (-l)</td>
<td>0.005</td>
<td>The lowest rate (Mbps) to probe at within chirp (-l)</td>
<td>0.005</td>
<td></td>
</tr>
</tbody>
</table>

Other adjustments by default

### Table 5: Pathchirp Configuration.

<table>
<thead>
<tr>
<th>Stab</th>
<th>Lan test bed 10/100 Mbps</th>
<th>Lan test bed wireless 54 Mbps</th>
<th>xDSL to xDSL test bed via VPN</th>
<th>xDSL to 3G test bed via VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Parameter</td>
<td>Value</td>
<td>Parameter</td>
</tr>
<tr>
<td>The experiment duration (secs) (-t)</td>
<td>100</td>
<td>The experiment duration (secs) (-t)</td>
<td>200</td>
<td>The highest rate (Mbps) to probe at within chirp (-u)</td>
</tr>
<tr>
<td>The highest rate (Mbps) to probe at within chirp (-u)</td>
<td>90</td>
<td>The highest rate (Mbps) to probe at within chirp (-u)</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>The lowest rate (Mbps) to probe at within chirp (-l)</td>
<td>1</td>
<td>The lowest rate (Mbps) to probe at within chirp (-l)</td>
<td>0.05</td>
<td></td>
</tr>
<tr>
<td>The number of packets per Jumbo packet (-J)</td>
<td>4</td>
<td>Other adjustments by default</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 6: Assolo Configuration.

<table>
<thead>
<tr>
<th>Assolo</th>
<th>Lan test bed 10/100 Mbps</th>
<th>Lan test bed wireless 54 Mbps</th>
<th>xDSL to xDSL test bed via VPN</th>
<th>xDSL to 3G test bed via VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Parameter</td>
<td>Value</td>
<td>Parameter</td>
</tr>
<tr>
<td>The experiment duration (secs) (-t)</td>
<td>200</td>
<td>The experiment duration (secs) (-t)</td>
<td>200</td>
<td>The highest rate (Mbps) to probe at within chirp (-u)</td>
</tr>
<tr>
<td>The highest rate (Mbps) to probe at within chirp (-u)</td>
<td>90</td>
<td>The highest rate (Mbps) to probe at within chirp (-u)</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>The lowest rate (Mbps) to probe at within chirp (-l)</td>
<td>10</td>
<td>The lowest rate (Mbps) to probe at within chirp (-l)</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Other adjustments by default

### Table 7: Statistics of tested tools on Lan test bed 10/100 Mbps.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Number of measurements (N)</th>
<th>(\bar{X}) (Mbps) (\sum_{i=1}^{N} (X_i - \bar{X})^2)</th>
<th>(\delta) with probability 68%</th>
<th>Relative error of tool ((n)) (*100%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DietTopp</td>
<td>15</td>
<td>68,286</td>
<td>146,755</td>
<td>0.841</td>
</tr>
<tr>
<td>Pathload</td>
<td>15</td>
<td>93,382</td>
<td>2402,649</td>
<td>3,382</td>
</tr>
<tr>
<td>Iperf</td>
<td>15</td>
<td>94,405</td>
<td>0,191638</td>
<td>0.030</td>
</tr>
<tr>
<td>PTR</td>
<td>15</td>
<td>58,922</td>
<td>0,485346</td>
<td>8,357</td>
</tr>
<tr>
<td>IGI</td>
<td>15</td>
<td>60,694</td>
<td>0,822,416</td>
<td>5,265</td>
</tr>
<tr>
<td>Stab</td>
<td>15</td>
<td>53,572</td>
<td>17,904,62</td>
<td>0,292</td>
</tr>
<tr>
<td>Pathchirp</td>
<td>195</td>
<td>86,949</td>
<td>3503,902</td>
<td>0,342</td>
</tr>
<tr>
<td>Assolo</td>
<td>17</td>
<td>70,809</td>
<td>1203,007</td>
<td>2,103</td>
</tr>
</tbody>
</table>

### Table 8: Statistics of tested tools on Lan test bed 54 Mbps.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Number of measurements (N)</th>
<th>(\bar{X}) (Mbps) (\sum_{i=1}^{N} (X_i - \bar{X})^2)</th>
<th>(\delta) with probability 68%</th>
<th>Relative error of tool ((n)) (*100%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DietTopp</td>
<td>15</td>
<td>5,883</td>
<td>0,918658</td>
<td>0,066</td>
</tr>
<tr>
<td>Pathload</td>
<td>16</td>
<td>6,430</td>
<td>48,86223</td>
<td>0,451</td>
</tr>
<tr>
<td>Tool</td>
<td>Number of measurements (N)</td>
<td>Mean ($\bar{x}$) (Mbps)</td>
<td>$\sum_{i=1}^{N} (x_i - \bar{x})^2$</td>
<td>$\delta_i$ with probability 68%</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------</td>
<td>--------------------------</td>
<td>---------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>DietTopp</td>
<td>15</td>
<td>0.287967</td>
<td>0.166467</td>
<td>0.028155</td>
</tr>
<tr>
<td>Pathload</td>
<td>15</td>
<td>0.394667</td>
<td>0.29723</td>
<td>0.021238</td>
</tr>
<tr>
<td>Iperf</td>
<td>15</td>
<td>0.383333</td>
<td>0.115301</td>
<td>0.023432</td>
</tr>
<tr>
<td>PTR</td>
<td>15</td>
<td>0.416667</td>
<td>0.155194</td>
<td>0.027185</td>
</tr>
<tr>
<td>IGI</td>
<td>15</td>
<td>0.416667</td>
<td>0.611263</td>
<td>0.053952</td>
</tr>
<tr>
<td>Stab</td>
<td>249</td>
<td>0.348000</td>
<td>0.749030</td>
<td>0.033483</td>
</tr>
<tr>
<td>Pathchirp</td>
<td>34</td>
<td>0.599853</td>
<td>0.218178</td>
<td>0.013945</td>
</tr>
<tr>
<td>Assolo</td>
<td>44</td>
<td>0.437045</td>
<td>2.820244</td>
<td>0.038608</td>
</tr>
</tbody>
</table>

Table 9: Statistics of tested tools on Lan test bed wireless 54 Mbps.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Number of measurements (N)</th>
<th>Mean ($\bar{x}$) (Mbps)</th>
<th>$\sum_{i=1}^{N} (x_i - \bar{x})^2$</th>
<th>$\delta_i$ with probability 68%</th>
<th>Relative error of tool (n) *100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>DietTopp</td>
<td>1</td>
<td>0.365497</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pathload</td>
<td>15</td>
<td>0.354000</td>
<td>0.209460</td>
<td>0.031582</td>
<td>8.921</td>
</tr>
<tr>
<td>Iperf</td>
<td>15</td>
<td>0.008</td>
<td>0.00028</td>
<td>0.001155</td>
<td>14.434</td>
</tr>
<tr>
<td>PTR</td>
<td>15</td>
<td>0.073267</td>
<td>0.041453</td>
<td>0.01405</td>
<td>19.176</td>
</tr>
<tr>
<td>IGI</td>
<td>No measurements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stab</td>
<td>No measurements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pathchirp</td>
<td>23</td>
<td>0.076261</td>
<td>0.00543</td>
<td>0.003276</td>
<td>4.296</td>
</tr>
<tr>
<td>Assolo</td>
<td>No measurements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 10: Statistics of tested tools on xDSL to xDSL test bed via VPN.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Number of measurements (N)</th>
<th>Mean ($\bar{x}$) (Mbps)</th>
<th>$\sum_{i=1}^{N} (x_i - \bar{x})^2$</th>
<th>$\delta_i$ with probability 68%</th>
<th>Relative error of tool (n) *100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>DietTopp</td>
<td>0.975</td>
<td>DietTopp</td>
<td>1.124</td>
<td>DietTopp</td>
<td>9.777</td>
</tr>
<tr>
<td>Pathload</td>
<td>3.622</td>
<td>Pathload</td>
<td>7.017</td>
<td>Pathload</td>
<td>7.111</td>
</tr>
<tr>
<td>Iperf</td>
<td>0.032</td>
<td>Iperf</td>
<td>0.195</td>
<td>Iperf</td>
<td>6.034</td>
</tr>
<tr>
<td>PTR</td>
<td>10.768</td>
<td>PTR</td>
<td>3.807</td>
<td>PTR</td>
<td>8.641</td>
</tr>
<tr>
<td>IGI</td>
<td>8.676</td>
<td>IGI</td>
<td>13.845</td>
<td>IGI</td>
<td>12.959</td>
</tr>
<tr>
<td>Stab</td>
<td>0.545</td>
<td>Stab</td>
<td>0.937</td>
<td>Stab</td>
<td>1.001</td>
</tr>
<tr>
<td>Pathchirp</td>
<td>0.350</td>
<td>Pathchirp</td>
<td>1.892</td>
<td>Pathchirp</td>
<td>2.325</td>
</tr>
<tr>
<td>Assolo</td>
<td>2.970</td>
<td>Assolo</td>
<td>0</td>
<td>Assolo</td>
<td>8.834</td>
</tr>
<tr>
<td>Ubiquiti Networks</td>
<td>2.623</td>
<td>Ubiquiti Networks</td>
<td>0.503</td>
<td>Ubiquiti Networks</td>
<td>0 no measurements</td>
</tr>
<tr>
<td>NetStress</td>
<td>2.527</td>
<td>NetStress</td>
<td>1.051</td>
<td>NetStress</td>
<td>0 no measurements</td>
</tr>
</tbody>
</table>

Table 11: Statistics of tested tools on xDSL to 3G test bed via VPN.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Relative error of tool (n) *100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>DietTopp</td>
<td>0 (only one measure)</td>
</tr>
<tr>
<td>Pathload</td>
<td>8.921</td>
</tr>
<tr>
<td>Iperf</td>
<td>14.434</td>
</tr>
<tr>
<td>PTR</td>
<td>19.176</td>
</tr>
<tr>
<td>IGI</td>
<td>No measurements</td>
</tr>
<tr>
<td>Stab</td>
<td>No measurements</td>
</tr>
<tr>
<td>Pathchirp</td>
<td>4.296</td>
</tr>
<tr>
<td>Assolo</td>
<td>No measurements</td>
</tr>
<tr>
<td>Ubiquiti Networks</td>
<td>No measurements</td>
</tr>
<tr>
<td>NetStress</td>
<td>No measurements</td>
</tr>
</tbody>
</table>

Table 12: Summary of Relative Errors of tested tools for all test beds.
Application Provision over the Future Internet Architecture

L. Panos¹, A. Papadakis²

¹ Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: p-lazaros@hotmail.com

² Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: andreas.papadakis@gmail.com

Abstract

This paper discusses the application provision over the future internet architecture with focus on Fi-Ware, which is an evolving Cloud Operating System based on OpenStack, that provides infrastructure and tools to application developers. Furthermore to Fi-Ware analysis on the respective fields of Virtualization, Cloud and IoT, we developed a Service Model that combines features of a Cloud OS and a microcontroller development board (Arduino), so to provide environmental conditions over the internet. On the last part we are evaluating the results from the conducted tests over the Service Model and we are proposing a future work.

Index Terms—Fi-Ware, OpenStack, Virtualization, Cloud, IoT, Arduino

1. Introduction

The new era of ubiquitous devices with high computational power and sensors that are infiltrating the market and moreover the everyday activities of humans, in combination with the Internet architectures that have been developed the last years, such as Virtualization and Cloud, led scientists and private sector companies to focus on a new approaches of application provision over the future internet architectures. On this document we will expose the architecture of the evolving Platform as a Service (PaaS) Fi-Ware, which a project that runs under the Future Internet Public Private Partnership (FI-PPP) program of the European Union and the Private Sector [1]. Additionally we are going to develop a Service Model, based on Fi-Ware platform and respectively on Microcontroller with interconnectivity options and environmental sensing capabilities, such as temperature and luminance. With this Service Model we focus to provide to the user or developer the latest values of the sensors, over the internet, with respect to Internet of Things (IoT). On the last part of this paper we will evaluate the developed system responses with respect to the Fi-Ware infrastructure.

2. Similar work and tools that we will use

Despite the fact that Fi-Ware is an evolving platform, some projects have been under development. From the perspective of our work, ENVIROFY [2] has an interesting approach on the field of provisioning the environmental conditions over the Fi-Ware
platform, but we are focusing to the implementation of simple deployed devices, such as Arduino [3], with minimum code and transmitted data over the internet, always with respect to availability, scalability and security.

The methodology that we will follow has two parts and contains literature study (Journals, Books, Periodicals, Fi-Ware platform, etc.) as a Secondary research and the second part is the Primary research, with the development of the Service Model, observing the real data that produced and evaluation of the results. The tools that we are going to use are, Fi-Lab as Cloud Operating System, Putty for secure connection with the Virtual Machine (VM), Arduino Development Environment for programming the Arduino device, RESTful Clients to observe the data, Microsoft Visio 2013 for Figures and diagrams and Fritzing for electronic diagrams.

3. Virtualization and Cloud

One of the main technologies that boost the creation of Cloud Infrastructures the last years, is Virtualization. With this technology, which provides separation of hardware from Operating Systems (OS) or applications, usually with proper software which is called Hypervisor, Datacentres or any PC can run multiple VMs with different OS. Those VMs are separated (usually called on sandbox) and they cannot see each other applications or programs [4]. At this point we need to mention that Virtualization is not only applicable to OS, but also to the networking part and to storage. This separation of hardware and OS gives the advantage of better resource allocation in terms of OS, networks, storage and Power consumption.

From the perspective of our work we will focus mainly on the cloud as a services, as they depict on Figure 1. We will describe briefly the three main layers from bottom to top.

![Figure 9: Cloud Service Pyramid.](image)

Infrastructure as a Service (IaaS) represents the hardware part of Cloud with servers, storage and networking equipment. A Hypervisor is responsible to handle all of this hardware equipment and the VMs respectively. Because the scale of this part could be very large, pools of Hypervisors work in cooperation so to provide to the system stability and scalability, always with respect to security and availability. Usually IaaS are based on Datacentres and by using Hypervisors the procedure to activate, deactivate or scale a VM is fast and eliminates the factor of human error.
PaaS provides to user/developer the proper tools and environments, such as OS, Web-Servers or programming languages, so to be able to develop their applications. Because it relies on IaaS, can offer high computational power and scalability very fast. Another important advantage is the fact that for complex applications that are using a lot of resources constantly or on-demand, the developers do not need to buy equipment (which probably would be expensive) and configure it, but only to use (or rent) the proper VM or combination of VMs on PaaS. Especially for testing purposes (e.g. Beta versions of applications) this characteristic can be very usefully, fast and with low cost. For the scope of our topic, Fi-Ware and more specific Fi-Lab is acting as PaaS in which we can deploy our VM. We will provide more details about Fi-Ware on other chapter.

Software as a Service (SaaS) provides to the user a ready to use software, which have been developed on top of PaaS, usually through a Web-page or through an application. By taking advantage of the features of PaaS and IaaS it can be reliable, fast deployed, always available, secured and scalable. One good paradigm of SaaS could be the e-mail services that are provided from companies like Google, Microsoft Hotmail, Yahoo and others. The user needs only a Web-browser or an application, to login to their e-mail and he/she does not need to configure anything else.

4. Internet of Things

The combination of ubiquitous devices with sensors and their capability to transfer those data through different types of networks is the new era of Internet of Things (IoT) [5]. With the ability to capture environmental or not conditions and transfer them through networks (e.g. Internet) the provided data can be very useful for monitoring or further processing. IoT can be considered as a container of networks, computational power and electronic devices with sensing capabilities that should be bond together to provide the desired result [6]. This means that IoT cannot be addressed only from one perspective (e.g. only network) and need to combine all of them to achieve the proper outcome in application level. The most important characteristic of IoT is that can connect the physical entities to digital entities [7] and this could be the first step of interconnectivity of everything and why not, for the Internet of Everything (IoE).

5. Fi-Ware Architecture

Fi-Ware is an evolving PaaS that focus on the developers’ demands with respect to the future needs of interconnection. From the beginning of the project the Fi-Ware community choose to use non-vendor specific products and to implement everything with Open Source codes and OS. The main components of the Fi-Ware are the Generic Enablers (GE), which are reusable and easy to deploy tools for the developer. From the architectural perspective, OpenStack is the base on which Data Centre Resource Management (DCRM) has been developed and is one of the main architectural components of Fi-Ware. DCRM according to Fi-Ware provides some extensive features in comparison with OpenStack [8]. We will describe briefly both of them.
5.1. OpenStack

Is a Cloud Operating System that have been developed with Open Source code from National Aeronautics and Space Administration (NASA) and Rackspace Hosting [9]. It can handle huge amounts of computational power and storage over a networked environment, so to provide the proper tools to developers or users. The main components of OpenStack are the following:

Compute (or Nova) that is responsible to manage the resources of the system with the VMs and acting as Hypervisor

Networking (or Neutron) which provides Internet Protocol (IP) addresses and some extensive features, such as Virtual Local Area Network (VLAN), firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) to the VMs

Storage (or Swift) provides two types of storage data, Object storage which is responsible to handle static data (VMs, photos, e-mails) and it is horizontally scalable. Block storage is responsible to provide persistent blocks of storage to Compute and to users

Dashboard (or Horizon) is the Web interface of OpenStack that provides access to users or administrators, so to manipulate or run their Instances (VMs)

Shared Services are recently added to OpenStack and they contain the following five features/components. First is the Identity Service (or Keystone) which is responsible to provide Authorization and Authentication services to users and administrators. Second is the Image Service (or Glance) which is responsible to handle disk and Server images. Third is the Telemetry (or Ceilometer) and is responsible to provide ‘visibility’ on the usage of the services across the platform (Bandwidth, storage, CPUs, etc.). Fourth is Orchestration (or Heat) and provides Template-style environment to connect the cloud applications in an automated and easy way. Fifth is Database (or Trove) and provides to users access to databases without participating on complicated administrative tasks during the implementation.

A major characteristic of OpenStack is the flexibility of usage the aforementioned features in a combination or all of them depending on needs of each platform. Figure 2 illustrates the components connection diagram through OpenStack Application Programming Interface (API) (Orange and Green arrows) and the interaction of user/administrator with Dashboard. From Identity Service, depending on the access level that has been defined for each user, he/she can access OpenStack and can use the available resources that have been assigned to that level of user.
5.2. Data Centre Resource Management (DCRM)

As we already mentioned DCRM is the main structural component of Fi-Ware, it is based on OpenStack and provides to the infrastructure all of the aforementioned features plus some extended features that focus mainly on high availability of the VMs and optimized utilization of resources, with respect to heterogeneous environments and virtual networking, including the federation of infrastructure [10]. From the Figure 3 we can see the detailed communication between the components of DCRM and the interaction with user/administrator. All of them are communicating with a unify way through Open Cloud Computing Interface (OCCI) API which is a RESTful technique that uses the Hypertext Transfer Protocol (HTTP) with PUT, GET, POST and DELETE to transfer data [11].

The visible components to user/administrator are the Virtual Image, Server, Disk, Network and Flavor (can be matched with OpenStack features). The last one refers to the computational power options (CPU, RAM and HDD) that will be used for each VM. Those are the resources that user/administrator can use to deploy the desired application, always with respect to access level that have been assigned to each user through Identity Management Service.
6. Service Model

On the scope of this paper we will describe the requirements of the experimental Service Model that will be used over the Fi-Ware public infrastructure. The system should follow three main directions.

Produce real time data that comes from environmental (or not) conditions
Store the produced data
Share the stored data on demand

To achieve this we will use a system that will have a Producer, Broker, and Consumer as depicts on Figure 4.

The Consumer will be responsible to retrieve information from the Broker and represent them to users. The communication from Consumer to Broker is bi-directional because the Consumer would not be limited to one application only, but could be another Broker or another application or a combination of them that can update the values on the Broker. This role would be assigned to NGSI Updater, one freely available Fi-Ware Widget.

The Broker will be responsible to handle and share the stored values on demand and would be assigned to Publish/Subscribe Context Broker (version0.12.0) [12], one GE from Fi-Ware catalogues. This GE will be used, because it can provide a unify way to communicate with the other elements of the System Model through the NGSI-9 and NGSI-10 RESTful interfaces. Additionally it is using a Database to store the values that will receive from Producers or Consumers.

The Producer (IoT), in this design, will be responsible to collect the environmental conditions of temperature and luminance, transform them to proper readable values (from humans and machines) and transfer them to the Broker. This role has been assigned to Arduino Uno Rev.3 development board with temperature and luminance sensors and interconnectivity capabilities [13]. As we can see from the Figure 4 the communication from Producer to Broker is one way, because Producer on this stage of development does not need to receive any information, only to send the produced data.
Moreover with the requirements and the proposed design of this Service Model we need to consider the facts of scalability from the perspective of infrastructure and accessibility from the perspective of user/developer access.

7. **Implementation of the Service Model**

To implement this Service Model we will use Fi-Ware Public Cloud Operating System (Fi-lab) [14] to support the Consumer and Broker and Arduino Uno Rev.3 to provide the real time temperature and luminance values. The communication-connection between those three parts of the System Model will be through the NGSI-10 interface and the HTTP POST request that would be send to Broker, so to update the values of temperature and luminance or retrieve them. All of the codes on main bodies of the requests are in Extensible Markup Language (XML) format and they provide flexibility on requests depending on the needs of each application (e.g. update only the temperature or request only the luminance value).

7.1. **Deployment of Consumer**

For a Consumer we are going to use the NGSI Updater as we already mentioned. This is a Widget on the Fi-lab Marketplace and can be deployed by installing it on our Fi-lab Workspace. To connect it with the Broker we need to put the Public IP address of the Publish/Subscribe Context Broker, the port that will connect and the Entity ID that will monitor or update. We can use additionally any RESTful client to monitor or update the values of the specific Entity ID.

7.2. **Deployment of Publish/Subscribe Context Broker**

The deployment of Publish/Subscribe Context Broker can be done either on a stand-alone Server or in the Fi-ware Public infrastructure (Fi-lab). We are going to implement it on the Fi-lab so to be able to test the performance of the System Model and of Fi-Ware together. To launch an Instance on Fi-lab we should have an account for the platform (https://lab.fi-ware.org), create a key-pair to be able to connect securely on the Instance, allocate a Public IP so Producers Consumers and administrators be able to reach it, set the desired security profile by blocking/allowing IPs, ports and protocols and then connect to the running Instance through a Secure SHell (SSH) connection to modify and activate the Publish/Subscribe Context Broker [15] [16].

7.3. **Deployment of IoT Producer**

For the role of Producer we choose to work with Arduino Uno Rev.3 development board and the respective compatible components, because it provides flexibility in terms of sensors, interconnectivity and the developmental environment is user friendly. Additionally it can provide enough power and options for future expansion to the System Model. The complete list of the parts that we will use is the following.

Arduino Uno Rev.3
Arduino Ethernet Shield Rev.3
Breadboard
LM35 Temperature Sensor
Photocell LDR (Light Sensor)
Resistor 120 Ohms 5%
Eight Coloured Wires (Jumper wires)
RJ45 FTP shielded twisted 4 pairs category 5 Ethernet Cable
USB cable (programming and Power Supply)

All of them have been configured properly according to Arduino Open Source Code and with respect to the specifications of each component [13, 17-19]. Figure 5 illustrates the Producer components connection diagram.

![Figure 13: Producer components connection diagram.](image)

On the above Figure 5 we can see the Arduino Ethernet Shield Rev.3 (on top of Arduino Uno Rev.3), the Breadboard that has the luminance sensor with the resistor (on the left) and the temperature sensor (on the right). All of them are connected to Arduino Uno Rev.3 through the Jumper Wires and are manipulated by the same board, so to provide the values of temperature and luminance to the Broker.

The setup of the Producer, designed to send data to Publish/Subscribe Context Broker every five minutes, so to use minimum network bandwidth, but this can be changed and the Producer can be send data real time in less than a second (depend on the bandwidth of Internet connection and on the time of TCP session establishment).

8. Results and Evaluation

We have separated the evaluation of the results in four areas, in which we are mainly focus on the functional part of the Service Model (including Fi-Ware), the scalability...
perspective, the security issues and we compare the Cloud-based Service Model infrastructure with a non-Cloud-based.

8.1. Functionality

From the functionality perspective, the Service Model that we have designed and developed is working without any issue and is capable to provide environmental values of the Producer to Consumer, through the Broker and most important is that Producer and Consumer are not communicate each other directly. This is an advantage, because with separation of the communication we can have different types of applications developed with different tools and respectively different types of producers that are using different programming languages. All of this diversity can be handled by the Publish/Subscribe Context Broker.

To evaluate the system functionality we have conducted two tests, one for the temperature sensor (Table I) and one for the luminance sensor (Table II) since they are working independent. Moreover for the evaluation period, we have changed the frequency of the Producer to send the data in real-time without delays and we interfere the environmental conditions by changing them near to the respective sensor.

<table>
<thead>
<tr>
<th>Real Room Temperature</th>
<th>Interfered Temperature</th>
<th>Measured Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>25</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>25</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>25</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>25</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>25</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>25</td>
<td>27</td>
<td>27</td>
</tr>
<tr>
<td>25</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>25</td>
<td>29</td>
<td>29</td>
</tr>
<tr>
<td>25</td>
<td>30</td>
<td>31</td>
</tr>
</tbody>
</table>

*Table 3:* Results from the test of the Temperature sensor (°C).

During the temperature test we were measuring the temperature near to the sensor with a secondary digital thermometer and we noticed that except from the values of 14, 18 and 30, that the Producer measured +1°C, all the others were same. From this evaluation we can deduce that the accuracy of the temperature sensor is acceptable, because the divergence on those three values was not so big.

<table>
<thead>
<tr>
<th>Real Room Luminance</th>
<th>Interfered Luminance</th>
<th>Measured Luminance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daylight</td>
<td>Daylight</td>
<td>278</td>
</tr>
<tr>
<td>Daylight</td>
<td>Covered sensor</td>
<td>25</td>
</tr>
<tr>
<td>Daylight</td>
<td>Semi covered sensor</td>
<td>98</td>
</tr>
</tbody>
</table>
Table 4: Results from the test with Photocell sensor (lux).

<table>
<thead>
<tr>
<th>Daylight</th>
<th>Flashlight 30 cm distance</th>
<th>407</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daylight</td>
<td>Flashlight 10 cm distance</td>
<td>760</td>
</tr>
<tr>
<td>Daylight</td>
<td>Flashlight 1 cm distance</td>
<td>1008</td>
</tr>
</tbody>
</table>

During the luminance test we noticed the changes that are illustrated on Table II. From the results and the respective specifications of the photocell [19] we can see that it has a relevant accuracy, but most important was the immediate response on the environmental change.

All of the results have been double checked through the Serial connection that Arduino Development Environment provides and from the Consumer. With this way we were verifying additionally that the last readings from the sensors were saved on the Broker.

At this point we need to mention that the only functional issue that we have faced, happened once on the Fi-lab, during the backup (Snapshot) of the Broker (VM), the task under the Instance tab was for more than 24 hours on Snapshot state, without making a Snapshot and without letting us to make any other change on the Instance through the Web interface. Moreover at the same time the Broker was working and we were able to access the Instance through SSH and manipulate it.

8.2. Scalability

Due to the architecture of Fi-Ware, which is based on OpenStack, we can understand that is fully scalable in terms of infrastructure. From the viewpoint of Publish/Subscribe Context Broker the scalability is one of the main characteristics of this GE. It has the capability to create and participate on a complex system of Brokers that are interacting each other with data records according to application needs. The combination of Fi-Ware features, such as Public IP and backup with Snapshot, with the capability of Broker to collaborate with other Brokers, provides high scalability to the application. With this way, the system can be implemented on a Public Cloud OS (e.g. Fi-lab), on a Private Cloud OS (e.g. rented space on a Datacentre), on a single Server with internet connectivity or in combination (Hybrid implementation) so to provide the desired amounts of computational power, availability, scalability and security.

From the perspective of Producer, the code can be replicated and can be used on different Producer (but with the same specifications), by only changing on the XML body of the HTTP POST request the IP address of the Producer and the Entity ID that we want to monitor (e.g. Room_Test_1). From the Consumer point of view, it can participate on the scalability of the system by changing the respective Entity ID on the XML body of the HTTP POST request. The only prerequisite is that all of the Producers and Consumers should be connected on the same Broker or pool of Brokers. With this way can be created an environmental (or not) monitoring system of tens or hundreds of Producers and Consumers, in short period of time and with minimum effort from the developer.
8.3. Security

The security of communications and data is a major area that every user/developer should focus on. For the developed Service Model, the security can be divided on two parts. The first part associated with the security of infrastructure and since Fi-lab is using secure protocol for the Web interface (HTTPS) and respectively we need to use SSH with our unique key-pair (that have been created from Fi-lab) to have access to the Instance (Broker), we can deduce that all of the connections are secured.

The second part involves the security of data that are transferred from Producer to Broker and from Broker to Consumer respectively. Because the version 0.12.0 of Publish/Subscribe Context Broker that we are using for the Service Model is under development, does not provide any stable feature of data encryption over the communication channels. This issue can be considered as a very important because all of the data are transferred through the internet unencrypted and thus can be under attack easily. According to Fi-Ware, in the future they will add encryption features for the communication between Producers, Brokers and Consumers.

8.4. Comparison of Service Model implementation with a non-cloud based system

As we already have mentioned Fi-Ware is a Cloud OS that provides resources and tools for application development, with respect to scalability, availability and security. All of those resources and tools can be managed and manipulated through a Web interface or through a remote access on VMs. At this section we will compare only the Broker and not the Consumer and Producer, because both of them are interacting with the Cloud OS, but are working independently.

To deploy our Service Model to a traditional (non-cloud) system the least parts that we should have are a Server, OS with proper configuration and Internet connectivity. All of them have a high cost comparing to the ready to use infrastructure of Fi-Ware and additionally the time of configuring the devices will be much more. Moreover to achieve high availability and scalability for a non-cloud based system it would be a complicated procedure and most probably will need a lot of effort and higher cost.

From this brief exposure we can deduce that the main advantages of application development over Cloud-based OS are the high availability and scalability with respect to security and low cost of implementation.

9. Conclusion

On this paper we dealt with the application provision over the future internet architecture and especially with Fi-Ware platform. From the evaluation of the results we can conclude that Fi-Ware, despite the fact that it is a new evolving Platform, it is capable to provide efficiently enough to developers the tools and infrastructure, so to be able to address the demands of the new era of cloud-based applications. Additionally we would like to propose as a further work, the expansion of the Service Model with more Producers and connection of Publish/Subscribe Context Broker with Big Data analysis server so to process the values and provide them through a
graphical environment. All of them with respect to security in data communications, availability and scalability.

Appendix

Figure 14: IoT Producer during the evaluation period.

Figure 15: Consumer with temperature value
Figure 16: Consumer with luminance value.

References


Deployment of video analysis capabilities in the compressed domain using FI-ware

D. Stathakopoulos¹, A. Papadakis²

¹ Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: stathakopoulos_d@yahoo.gr

² Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: andreas.papadakis@gmail.com

Without doubt, the evolution of internet has created a huge traffic potential, especially in terms multimedia traffic. However, as the amount of multimedia traffic constantly rises, respective demands for video content analysis have been observed. The emergence of internet of services, cloud computing and future internet platforms has created a promising perspective for innovative application deployment. In this direction, FI-ware platform provides a wide range of services known as generic enablers (GEs). Compressed domain video analysis (CDVA) GE offers an alternative video analysis approach compared to traditional video analysis techniques. This thesis attempts to present and exploit CDVA GE capabilities in order to evaluate video analysis functionality in the context of future internet platforms.

1. Introduction

There is no doubt that Internet has been established as an everyday life need likewise to electricity or water. The underlying evolution of computing and telecommunications including the massive increase in mobile devices as well as the excessive penetration of social media has led to massive data generation. However, the vast majority of traffic is considered as multimedia traffic, which is expected to further increase over the next years. In this respect, in order to since multimedia applications are considered as bandwidth-intensive, consuming massive computing resources, many compression standards have been deployed so as to enable efficient multimedia transmission over public and private networks as well.

As long as the amount of multimedia traffic constantly increases, the need for effective multimedia analysis increases in a proportional manner, aiming to extract meaningful information from the exchanged multimedia content. However, most of video analysis methods are able to perform solely on the uncompressed domain increasing the operational complexity level. Hence, scientific community arguably focuses on the deployment of video analysis techniques able to deliver effective services in the compressed domain.

As the internet constantly evolves aiming to address future requirements, the Internet of Services (IoS) has been proposed envisioning a unified platform of available services. In the context of IoS, cloud computing has introduced a novel approach, providing software and hardware resources “as a service”. Thus, cloud-based approaches have been recently proposed focusing on massive multimedia traffic.
processing in an effective manner. In this sense, FI-ware platform has been developed aiming to provide a wide range of application development tools in a cloud based model. The particular work focuses on FI-ware functionality in terms of video analysis exploring Compressed Domain Video Analysis Generic Enabler (CDVA GE) capabilities.

2. Video Analysis

Nowadays, the evolution of telecommunications in respect to mobility as well as has created a new potential for services that exploit large amount of data. In this sense, the significant rise of smart mobile devices, the evolution of social media as well as the emergence of content providers have affect the exchanging traffic over the internet [13]. The particular amount of data is huge considering that may correspond to content created by physical entities or other applications, sensors etc. Moreover, video traffic is expected to comprise the vast majority of internet traffic over the next years. To this extent, according to a recent research it is estimated that about 69% of global traffic will consumed by video applications while video delivery networks will provide more than 60 percent of global video traffic by 2017 [8]. As enormous amounts of multimedia traffic are expected to be the dominant traffic over the next few years, it is apparent that applications should be able to exploit this potential by analyzing and processing media content.

With the intention of efficiently utilize transmission media, advanced video compression standards have been developed, aiming to offer high quality video services in a bandwidth effective manner [21]. In this respect, the majority of video applications rely on block-coding methods, especially hybrid-block coding, due to its significant compression performance. Figure 1 displays the main components of a hybrid video encoding scheme.

![Figure 1: Hybrid video encoder](image)

As video compression standards constantly evolve, video analysis field has been evolved in parallel, aiming to extract meaningful information by analyzing video content. In the context of video analysis methods, human vision constitutes an effective method which has been widely adopted in the near past. However, even though the particular approach has been widely adopted due to its reasonable effectiveness, it is
proved to be cost-ineffective since it depends on human factor, by employing monitoring personnel for event detection purposes. The specific limitation can be further extended, considering that as the number of video sources increase, a relative increment to the employed staff should be considered so as to preserve the intended effectiveness [19], [24].

The rapid emergence of video compression standards motivates the need to develop effective video processing schemes able to extract meaningful information from video content in an automated manner. The majority of them exploit the pixel domain implying that analysis procedures are performed comparing the values of each pixel in different successive frames [21], [19]. However, even though human interaction is not required, the actual pixel data recovery relies on decoding prior to analysis procedures. Thus, a complete decompress/process/re-compress cycle is required [21]. The specific limitation is very important considering that decoding process requires buffering resources as well as respective computational power and time.

Video processing in the compressed domain constitutes an alternative proposal able to perform efficient processing operations on compressed data. In particular, while conventional approaches require decompressing the bit-stream, processing the decoded frames, and re-encoding the result, CDP methods offer the ability to directly operate on the encoded bit stream, eliminating the need for decoding prior to analysis. The significant advantages of this approach rely on the reduced computational power and memory requirements leading to a corresponding reduced processing time required for the analysis procedure, and thus effective real time application support becomes feasible. Figure 2 displays compressed domain video processing.

![Figure 2: Compressed domain video processing [23]](image)

In the context of video analysis, most of applications rely on global change detection and moving object identification which comprise the key objectives of video analysis schemes [24]. CDVA GE provides both of these functions, processing video streams in the compressed domain.

3. **FI-PPP**

Without doubt, Internet has been evolved into a vital socio-economic factor of modern ages. Internet's massive growth was not solely influenced by the improvements related to the telecommunication infrastructure but also by the introduction of novel services such as the world wide web (www), e-mail etc. To this extent, motivated by the impact of internet, design and implementation of innovative as well as revenue-promising
services, has become a major point of interest for enterprises which invest large amounts of money on this direction [1]. The next day of internet introduces the web 2.0 concept which attempts to deliver software functionality over the web, in an “as a service” manner. In this sense, more and more companies including Google, Amazon and Microsoft have adopted the particular approach, introducing The Internet of Services (IoS) approach [4]. According to this proposal, the internet constitutes an interoperable framework, enabling collaboration between multiple services and resources [8].

In the context of IoS perception, Cloud computing has been established as a promising computing approach, providing software and hardware resources as a service. In particular, resources such as software-based applications, software development tools, networking and storage infrastructure can be delivered on demand over the internet [9]. Therefore, it is expected to make great impact on future internet deployment due to its attributes in terms of elastic service and resource provision, reduced requirement for infrastructure application development tools installation and maintenance, and finally enhanced service management and security potential [10].

Exploiting the IoS and Cloud computing perspective, Future Internet Public Private Partnership (FI-PPP), aims to provide an integrated platform oriented framework for advanced research and application deployment [14]. In particular, it includes software, networking, communication and virtualisation services with the intension of deploying large scale as well as real-world applications in a platform-based manner [15]. FI-PPP has evolved in three phases [16]. The initial requirements of the project were defined during the first FI-PPP phase, proposing eight use-cases, which even though are independent each other, their requirements are fulfilled exploiting services provided by the FI-PPP framework in a transparent manner [13]. In particular, the initial use-cases influence areas such as health, logistics, safety, environment, energy, transport, mobility, media & entertainment and agri-food [16].

4. FI-ware

In the context of FI-PPP, FI-ware constitutes one of its most prominent projects since it is considered as the foundation of the FI for European IT industry. According to [14], it was introduced as a consortium of top-class European Information and Communication Technology (ICT) organizations, including SAP, IBM, Telefonica and many others, which intend to provide a platform-oriented framework for the FI. In essence, FI-ware foundational companies intend to exploit the subject platform, so as to promote their own business strategy [13].

FI-ware functionality relies on operational building blocks known as Generic Enablers (GEs). By definition, GEs consists of a set of software components and a set of APIs and interoperable interfaces in order to deliver specific functionality in an “as a service” manner [1]. The significant advantage of FI-ware approach relies on the efficient application development, based on service functionality provided by the available GEs. Hence, integrated services can be composed by combining multiple GEs, implementing in this way IoS perspective [8].
With the intention of covering a wide range of technical fields, GEs are grouped into six main categories. In particular, GE usage areas are Applications/Services Ecosystem and Delivery Framework, Cloud hosting, Data/Context Management, Interface to Networks and Devices (I2ND), Internet of Things (IoT) Services Enablement, and Security [13].

The significant advantage of GE utilization in application development process relies on the facility of deploying innovative applications in a timely manner, based solely on the offered functionality rather than on service development or infrastructure requirement issues [13]. Moreover, the offered modularity constitutes another critical advantage since each GE component can be upgraded without affecting other interconnected GEs, while optimization processes are applied exclusively at the provider side in a transparent manner from end users [11]. Furthermore, GEs offer reusability benefits, since each GE can be exploited in many different applications, enabling multiple instances of the same service in a reusable manner [13]. Finally, since GEs operate in a cloud based environment, dynamic as well as real-time resource provision becomes practical, enhancing the underlying adaptability [4].

5. Compressed domain video analysis GE

As enormous amounts of multimedia traffic are expected to be the dominant traffic over the next few years, it is apparent that applications should be able to exploit this potential by analyzing and processing media content. To this extent, Compressed-Domain Video Analysis (CDVA) GE, developed by Siemens, provides robust video analysis functionality “as a service” through FI-ware platform [19]. In particular, CDVA is included in Data/Context Management GE, offering an integrated framework, focusing on real-time video analysis in the compressed domain. According to CDVA GE specifications, the particular GE is recommended for telecom industry applications so as to process video content provided by mobile users. Furthermore, CDVA potential can be exploited in point of interest identification, social services and by surveillance industry as well, in order to automatically monitor detect critical events [21].

In order to effectively process video in the compressed domain CDVA GE consists of a set of interconnected components. In particular, CDVA consists of the Media Interface, Media Analysis, Metadata Interface, Control, and the API components [20]. Figure 12 presents graphically the CDVA functional components.
In particular, CDVA GE provides a Media Interface in order to support multimedia stream reception [19]. Media Interface provides interfaces for both stream-lined multimedia as well as already stored multimedia files. Furthermore, it is capable of handling multiple parallel RTP sessions while different multimedia formats are supported. Media Analysis component constitutes the most important component of CDVA architecture [19]. In particular, it processes video received by the Media interface, in respect to event detection and moving object detection supporting real time and non real-time processing modes. The algorithms used for the aforementioned operations are presented in detail in [26] and [27] respectively. Metadata Interface processes the output of Media Analysis component generating notifications based on the analysis results [19]. Finally, CDVA offers a set of supplementary interfaces for external configuration and control purposes. In particular, the API component provides a RESTful interface so as to allow external users submit their requests in a HTTP form [19], [20], [22] while it provides a Control component which is responsible for generation and management of the active CDVA instances.

6. Implementation

The particular thesis attempts to assess CDVA GE functionality by analysing input stream in respect to global change detection and moving object detection. According to the proposed methodology, a CDVA GE instance should first be created from FI-lab. In order to ensure optimal performance, CDVA GE image is installed on a virtual machine providing two VCPUs and 2GB RAM. In order to make CDVA GE instance accessible for configuration as well as for input streaming purposes the following security concepts should be considered. First of all, REST-ful API provides HTTP-based interaction with CDVA GE, the instance should be configured so as to allow traffic on port 80 [29]. Furthermore, in order to enable video stream reception, the corresponding port should be opened. CDVA GE is able to process traffic employing Real-Time Streaming Protocol (RTSP) which operates on port 554 and thus the particular port should be accessible [29]. However, RTSP relies on Real-Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP) using random TCP ports within 49152 and 65535 ranges [29]. Finally, in order to enable remote access to CDVA GE instance, secure shell (SSH) is employed which operates on port 22 [22].
As soon as, a server image is instantiated and properly configured, it is feasible to initiate CDVA GE instances so as to enable video analysis process. In particular, configuration is based on a set of REST-ful operations provided in an xml-based form through the REST-ful API. The key objective of the CDVA GE evaluation process relies on stream reception from a single source in order to detect global changes or to detect moving object. Therefore, a single CDVA GE instance should be created. Furthermore, in order to receive analysis results, a sink should be created and linked to the CDVA GE instance. Upon linking CDVA instance to a sink, the instance should start performing media analysis. As soon as the analysis finishes, the underlying CDVA GE instance should be terminated and the corresponding sink should be removed. Figure 25 presents the sequence diagram of the proposed CDVA GE evaluation use case.

Figure 4: CDVA instance sequence diagram

As long as the remote CDVA server becomes accessible, an RTSP streaming server as well as a web server should be employed as an RTSP source and as a Sink respectively. Figure 26 shows the underlying topology.

Figure 5: GE use case sequence diagram
At the local network side, VLC software serves as an RTSP streaming server while a mongoose web server provides web server functionality in order to receive analysis output. VLC is configured so as to capture real time video from a pre-installed video camera. The underlying video is encoded according to the H.264-AVC standard while it is streamed using RTSP. Along with fig.5, a user is able to communicate with remote CDVA server through REST client software since remote server provides a REST-ful API for communication purposes. In particular, a web interface accessible on port 80 is provided, enabling CDVA GE instance creation and configuration using simple HTTP requests. Upon instantiating a new CDVA GE instance, parameters as RTSP stream URI as well as the URI of the Sink, should be provided to the CDVA GE instance. Subsequently, in order to analyse streaming media, CDVA GE acts as an RTSP client, requesting an RTSP session initiation from the RTSP streaming server. In most of cases, RTSP server receives session initiation requests on port 554. As long as the RTSP session is established, CDVA GE receives video stream in an RTP form. For RTP stream transmission, random UDP ports between 49152 and 65535 port ranges are used [29]. However, in cases of RTSP interleaved mode, it is possible to transmit RTP stream using the already established RTSP session which is based on TCP.

CDVA GE instance creation constitutes a primary issue in the particular video analysis process. Hence, a createInstance request should be sent to the remote server in order to create a CDVA GE instance. The specific request relies on HTTP POST method including three parameters in order to specify video analysis procedures and the input RTSP stream URI. As soon as the CDVA GE instance has been created, it is feasible to configure analysis parameters which in fact are related to the employed algorithms described in the previous section. To this extent, a configureInstance request, which is based on HTTP POST method, can be employed in order to specify the analysis parameters according to the event detection and moving object detection algorithm specifications CDVA GE should be aware of the Sink URI where the analysis results will be posted. Since a local web server serves as a Sink in the experiment, an addSink request should be used to inform CDVA GE about Sink URI. Moreover, in cases that multiple recipients of the analysis results are required, multiple sinks can be configured to receive notifications from the same CDVA GE instance. Each sink is identified by a unique ID number. Upon creating a CDVA GE instance and a corresponding sink, the analysis process is can be initiated. In this sense, a startInstance request should be sent to the remote server. The particular request relies on HTTP PUT method specifying the CDVA GE instance ID.

As soon as the analysis scope has been fulfilled, the CDVA GE instance should be stopped. In this case, based on HTTP PUT method, a stopInstance request should be sent, specifying the CDVA GE instance ID. The analysis results are available in the local web server log file. In particular, the xml based notifications have been posted to the specific log file as HTTP POST requests each time a critical event was detected during the analysis process. Prior to CDVA GE instance removal, all related Sink should be removed as well. Therefore, based on HTTP DELETE method removeSink and destroyInstance requests should be sent to the remote server respectively.
7. Discussion

In order to assess CDVA GE functionality, it is apparent that a detailed analysis of evaluation results should be provided. First of all, FI-ware platform provides a simplified process in order to instantiate a server instance. The majority of commercial video analysis applications rely on local infrastructure installation. In particular, a local server machine and video analysis software should be hosted locally so as to analyse the received traffic. However, server installation and video analysis software configuration requires expert knowledge while they constitute an additional expense. Furthermore, regular maintenance procedures should be applied at the local side in order to keep hardware and software up-to-date. On the other hand, since CDVA relies on cloud based model the aforementioned limitations have been overcome enabling server installation and CDVA GE software in a simplified manner. Furthermore, infrastructure maintenance and update are responsibility of FI-ware development parties without any invocation required from the end user side. Furthermore, communication with the remote CDVA GE is facilitated since it is based on simple HTTP requests which can be posted using commodity web browsing software.

However, even though CDVA GE instance generation was successful, it failed to perform video analysis operations during the evaluation process. In essence, CDVA GE developers have tested CDVA GE functionality exclusively at local level, by installing it as a software component on a local computer and input data from a local web camera. Unfortunately, CDVA GE has not been tested yet in cloud-based environments where it is accessible only from remote networks. The key problem was an internal server error which corresponds to failure in establishing an RTSP connection and hence to receive video traffic remotely. The key problem was an internal server error which corresponds to failure in establishing an RTSP connection.

At the time of writing this thesis, the particular issue is under investigation and it is expected to be solved on later CDVA GE versions.

Furthermore, according to CDVA GE specifications, the particular version does not support integration with other GEs. Hence, an integrated video analysis application able to include more GEs is not yet feasible. In this reference, instead of posting the analysis results into a web server log file, it would be more effective to use another GE as a Sink. In this way further analysis and meaningful information extraction would be feasible since notification messages are in an xml-based form. Data/context management framework provides a set of GEs, which are able to collect, processing and publishing large scale data. Therefore, it would be sensible to exploit its enablers for further processing of video analysis results, in the context of an integrated video analysis application.

Finally, the lack of other GEs enablement, raise security concerns since no authentication processes can be involved in CDVA GE management process. In other words, possible attackers are able to interact with CDVA GE RESTful API by simply knowing the remote server instance IP address, since no authentication or additional security processes are employed. Therefore, future upgrade of CDVA GE should focus on this direction, so as to support enablers from the FI-ware security framework is
essential in order to provide an integrated video analysis application based on CDVA GE and FI-ware platform.

8. Conclusion

According to the assessment results, even though the video analysis operational framework is by far simplified, facilitating setup process and significantly reducing setup time, there are issues which establish CDVA GE proposal as an ineffective solution for remote video analysis. In fact, cloud-based video analysis is still on primitive stage, hence more researches should focus on this direction in order to achieve the expected performance. To this extent, along with the assessment, the key limitation identified, deals with the inability to establish RTSP sessions and consequently RTP session for video content reception. Future work should focus on enhancing CDVA GE functionality focusing in effective RTSP session establishment as well as on the development of an integrated video analysis application able to combine multiple GEs of FI-ware platform.

References

IPv6 in an Untrusted World

N. Xifaras\textsuperscript{1}, H. Katopidis\textsuperscript{2}

\textsuperscript{1} Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: nerosthian@hotmail.com

\textsuperscript{2} Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: hkatopodis@yahoo.com

Abstract

After nearly three decades Internet Protocol version 4 (IPv4) is ready to step out for its successor IPv6. New address scheme, simplified header format and mandatory use of IP security (IPsec) mechanism are a few specifications of the new protocol. IPv6 deployment worldwide is still an ongoing procedure and fear for security breach has always been a crucial topic. IPv6 introduces several threats and vulnerabilities. Paper presents classification of threats and with the help of Graphic Network Simulator (GNS3) a Testbed simulation is created, with tools THC-IPv6 attacking toolkit and Scapy attacks will be performed in the lab in extension headers and Internet Control Message Protocol version 6 (ICMPv6) to show in an understandable way how easy is for a malicious user to attack IPv6 protocol and targets. Also countermeasures are indicated to mitigate attacks and threats.

Keywords-IPv6-DoS-IPsec-security,ICMPv6,NDP

1. Introduction

Internet Engineering Task Force (IETF) development IPv6 [1] as an evolution to the IPv4 protocol and was designed to overcome drawbacks of its ancestor and update it to the needs of nowadays technology. Transition to the new era has started and 6th June of 2012 was the day that IPv6 was officially launched. This movement was supported from many tech companies and universities [2]. Due to the fact that both protocols are related, most security threats and attacks from IPv4 can also be harmful for IPv6 networks and devices. IPv6 security mechanisms improve many topics and reduce drawbacks but also new types of threats and security issues are introduced. Currently IPv6 is not the basic target for malicious users but as the adaption continuous this will change. Today there are several tools available that have been developed to leverage IPv6 protocol. Tools like THC-IPv6 attacking toolkit [3] and scapy [4] can be used to harmful IPv6. Paper is organized as follows: Section 2 includes a brief understanding of IPv6 specifications. Section 3 mentions Testbed, section 4 threats and vulnerabilities along Testbed. Last section of paper closes with some conclusions.
2. **IPv6 Specifications and features**

IPv6 offers a 128 bit address space length which can be considered one of the main advantages over IPv4 that offers a 32 bit address space. IPv6 offers three types of addresses, presented in RFC 4291 [5]. A unicast address recognizes an interface. An anycast address can identify a group of interfaces, packets sent to an anycast address is to be delivered to the closest interface. Multicast addressing identifies a group of interfaces like in anycast but with one difference, packets destined to multicast addresses are delivered and received by all interfaces in the multicast group. IPv6 header format offers a simplified protocol header. It expands the address field from 32 to 128 bits, offers a fixed length header of 40 bytes which result in faster IP datagram processing, also no fragmentation on router is performed and similarly checksum header is not included which reduces the cost of header processing and increases the routing speed. Field of options has moved into the next header field of IPv6 and its removal was the main reason for a fixed length [6]. Flow label makes it easier for routers to detect and categorize traffic streams. [7]. Furthermore IPv6 is using IPsec as its basic security mechanism that provides authentication, data integrity, confidentiality and encryption. IPv6 can offer stateless autoconfiguration (SLAAC), host can obtain IP address automatically or through a Dynamic Host Configuration Protocol (DHCPv6). IPv6 offers mobility and gives the ability to mobile users to maintain their connection when they are on the move [8]. ICMPv6 is crucial for overall functionality of IPv6 as it provides diagnostics and error reporting. Neighbor Discovery Protocol (NDP) replaces functionalities that are used in IPv4 like Address Resolution Protocol (ARP), and in addition is making use of five ICMPv6 messages, Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor advertisement (NA) and redirect specified in RFC 4861 [9], additionally NDP performs a series of functionalities like, prefix discovery, redirect, keep track of neighbors, discover neighbor routers and reachable neighbors also it is used to SLAAC configuration, discovery of duplicate address and notify hosts for a next hop determination to transmit their packets.

3. **Testbed**

The Testbed aims to show how easily is to harm extension headers and ICMPv6. Testbed examines extension headers field and ICMPv6. These two topics are addressed because ICMPv6 has a crucial role to the overall function of IPv6. Additionally extension headers are easily harmed with spoofed packets and malicious user can gain access to the network. Simulation is designed with the help of Graphic Network Simulator version 3 (GNS3) [10] and help us to emulate networks and work with virtualized machines and devices. Further GNS3 supports the Cisco IOS and it is an open source program available to several platforms. The testing simulation is designed by using a virtual router Cisco c7200 which supports the use of IPv6 features, and by using VMware workstation [11] it is possible to install several virtualized OS in our physical system, we have three OS in a private LAN network Windows 7, Ubuntu 12.04 and Backtrack 5 R3 that stands for malicious users. All OS in the Testbed are configured with IPv6 addresses, scapy [4] will be used to forge packets and THC-ipv6 attacking toolkit [3] attacks will be executed in the ICMPv6 field. With the help of packet analyzers like tcpdump [12] and Wireshark [13] we are able to capture traffic. Also eth0
stands for the interface that controls the Ethernet network interface card in our case eth0.

4. IPv6 threats and vulnerabilities

Extension header is a field that malicious users can use it in order to manipulate it and execute attacks. DoS, evasion of Intrusion Detection System (IDS) and firewalls, hidden harmful data within extension header are some threats that rise in this area.

4.1. Extension header threats

Hop by hop has to be examined through all intermediate nodes along the packets path while destination has to be examined only at the destination node. Hop by hop appear only once in an IPv6 packet but within it is possible to contain many options in any order, like PadN and router alert option. PadN must have a 0-byte payload, other than that means there is an error and this can be used by malicious users as a covert channel. With this he can deliver information within the network by moving the fields of the packet. Firewalls have to check whether the PadN contains other than 0s in the field or multiple padding options, in all cases it should drop these packets. Figures 1 and 2 shows an example to send messages within PadN options. A destination options header with three PadN messages is created. With the use of tcpdump [12] packet sniffer we are able to see in order to see IPv6 packets.

![Figure 1. Message with three different records.](image1)

![Figure 2. Three PadN records.](image2)

Router alert indicates to a router to investigate the contents of a packet header, malicious users can use it to cause issues with their performance by receiving a large number of packets that contain router alert hop by hop option. Figure 3 shows a router alert packet created with the help of scapy [4]. A packet RAlertPacket is created and the next header is 60 which indicate a destination option header that has a router alert option.
Some networks cannot transmit large packets so the use of fragmentation deems necessity as it divides large packet into smaller ones. Further fragmentation process is achieved only by end nodes and only these can form and reassemble fragments not routers. A malicious user can use fragmentation to execute attacks, for instance he can divide a packet into tiny fragments in order to avoid detection of firewall or IDS as it will look like legitimate, known as tiny fragmentation attack. Moreover due to the fact that IPv6 header chain is long enough it is possible the first fragment of a packet to not be included in IPv6 header chain, therefore firewalls are unable to verify first fragment which contains the header information and simply permits it to reach destination host. Additional another attack is overlapping fragmentation, which occurs when fragment A is overwritten from fragment B and vice versa, this derive from the fact that two fragments within the same IP datagram have offsets which overlap each other. This type is also used to avoid firewalls and IDS systems [14]. A fragment packet is created with scapy [4] and it is send to the destination address. IPv6 header is equal to 44 and specifies that a fragment header follows the IPv6 header, in figure 4 we see a parameter problem, this occurs due to the fact that the packet is less than 1280 bytes so it is not the final fragment and destination host response with an ICMPv6 error message with the parameter problem of an incorrect header. Malicious users can send an amount of packets and thus crushing destination host which sends back ICMPv6 error messages.

4.2. Countermeasures

Firewall has to block all site local scope addresses (ff05) as well as multicast in order not to expose IPv6 addresses outside the local network. Firewall should be able to
detect and block numerous echo request in order to avoid flooding within the network. Additional in order to prevent internal attacks the use of unicast Reverse Path Forwarding (Urpf) is critical. It is specified in RFC 3704 [15] and when it is enable routers inspect the source address of the incoming packets and forwards packets only if they can be reached from the interface the packet was received, therefore a malicious use inside the network will not be able to send spoofed packets hence in order to maximize security Urpf has to be activated on all interfaces internally. Moreover the PadN option should have only 0-byte payload otherwise it should be blocked. Router alert option has values between 0 and 35 anything between 36 and 65535 has to be rejected. Further fragments with less than 1280 MTU should be dropped. Additional the administrator could also block any extension headers that are not used with respect not to disable any usable extension header that is needed for the overall process.

4.3. Attacking ICMPv6

A router sends RA messages in order to inform all nodes on the path about its existence and its routes, now if a malicious user sends spoofed RA messages node are likely that they will select him as their default router as he dupe the hosts that are listening to RA messages resulting in exploitation of DoS and man in the middle attacks. With the help of THC-IPv6 attacking toolkit [3] we can send RA messages that public link-local IPv6 address form the malicious user as a default router, the following commands helps as to execute this attack, ./fake_router26 interface it sends advertisements every second to all multicast address on the local link. Figure 5 shows us the routing table of the Windows 7 machine before and after the attack hence with command netsh interface ipv6 route we can see 2 default routes with metric 16 and 256. Metric low is better. 16 points to bogus in backtrack and the other one in the router. The device is tricked and thinks that backtrack-malicious user is the default gateway and all packets are traveling through his link local address.

Additional a DoS threat known as bogus IPv6 prefix on link can be implemented by recommending IPv6 prefixes to assign IPv6 addresses for nodes. Malicious users can send RA messages which states that prefix is on link therefore hosts falsely will believe that this prefix is on link and will not send any packets for this prefix to the default router, for that reason host with the use of NS message will try to implement address resolution but then NS will not respond resulting in denying service to the malicious host. Malicious user by applying infinite lifetime to the bogus prefix can deny services to the sending host until it loses the state of its prefix list. Further in address
autoconfiguration with the use of RA message again a malicious user can state an invalid subnet prefix for usage by hosts to complete the procedure. Although the prefix is not valid a host will continue with the process of address autoconfiguration which results the correspondent packets not to be reachable by the host because of its invalid source address also known as bogus address configuration prefix [16], [17].

With the command kill_router6 from THC-IPv6 attacking toolkit [3] we can execute a DoS attack, moreover this attack sends RA messages from the spoofed IPv6 address of the default router with a lifetime of zero and tells all nodes to delete existing default route from their routing tables. As a result target user is trying to send all packets to the nodes rather than router and packets may not reach their destination since the destination is not an on link node. Traffic captured with Wireshark [13] can be seen in Figure 8.
5. RA Flooding

RA flooding attack produces a flood of RA messages with random IPv6 prefixes and MAC addresses forcing nodes to run SLAAC procedure, computers have SLAAC configuration enabled by default which results in calculating the IPv6 suffix and also update its routing table in order to accept messages. This method results in a DoS attack which exhausts the resources, especially in Windows OS like Windows XP, 7 even 8 the CPU reaches 100% of its performance and the system crashes or freezes and does not respond even when the attack has stop [18]. In addition to Linux, afterwards the attack the system can operate again, further major vendors like Cisco, Juniper were suffering from this attack which was found around 2008 [19], [20]. Further Sam Bowne and Matthew Prince [21] state that RA flood still exist in Windows and in OS like android of Google although distribution of Linux by Ubuntu has no flawlessness against RA flood.
6. **Duplicate Address Detection (DAD)**

IPv6 offer the ability to hosts to acquire an address through SLAAC procedure, DAD is a mechanism that prevents the use of same address twice in a network. When a host joins a network and has an address through SLAAC it sends a NS message to all nodes with multicast address in order to verify that no other is using it, when there is no reply it starts using it. A malicious user can perform DoS attack just by replying to DAD mechanism either by replying to the NS message with a spoofed NA message claiming that this particular address belongs to him or with a spoofed NS message which falsely pretends the DAD mechanism [22]. Command detect-new-ip6 can help as since it reports any new device that it sees. In figure 11 we can see one link local address and
two global addresses, one is reaching the device and the other two for the privacy extensions portion of IPv6. Command dos-new-ip6 listens for ICMPv6P DAD packets on the network, when it sees one then it will respond saying that this address exists and by this no host will be able to connect to the network. A malicious user can send NA messages in response to DAD NS messages with the command dos-new-ip6, Figure 13 show us the spoofed NA messages for each DAD NS message which results the target user not to obtain an address.

7. Countermeasures

To robust security and mitigate attacks IETF introduced SEND which is specified originally in RFC 3971 [23] and is updated in RFC 6494 [24]. The main principle is that a host must be configured with an “anchor” that will only accept routers with trustful certifications, as a result it mitigates spoofed RA messages. Cryptographic Generated Address (CGA) is used to protect messages that are related with neighbor and router discovery, timestamp and nonce options are used to thwart replay attacks [25]. Nevertheless IPsec can also provide solution to the NDP as nodes can use IPsec to protect ND messages. However RFC 3971 [23] indicates that “IPsec can only be used with manual configuration of security associations”. Furthermore rogue RA messages can be exposed with the use of IDS as long as it has a list with legitimate routers and hosts. Besides RFC 6105 [26] provides solutions on how a layer 2 device can block rogue RA messages. RA guard can be used in order to permit RA from switch ports where routers are linked in addition it has to filter RA that arrives on all other ports [27]. Additional open source programs like NDPMon [28] provide diagnostics and detect anomalies over NDP messages and ICMPv6 overall, similarly other useful programs are NDPWatch [29], rafixd [30] which are used to detect anomalies and not mitigate or block any attacks. RFC 4890 [31] proposes recommendations for filtering of ICMPv6 messages in firewalls. Therefore in ingress filtering firewall should accept all ICMPv6 that are function for the communication process in IPv6 and reject packets that contain special prefix in their source address. In addition to egress filtering, firewall should permit to send ICMPv6 packets that are crucial to proper communication and deny sending packets with special prefix in their source address.
8. Conclusion

In the Testbed we execute several attacks and show how easy is to perform attacks in IPv6 with the tools that we used. All attacks were executed from Backtrack5 R3 and all attacks were executed independently. Attacks were successful of their scope and hit their target also we notice in RA flooding that Linux distribution handles better the attack than Windows 7. Linux only generates a few IPv6 addresses and stops but then again windows 7 generate thousands and the system freezes. Countermeasures for mitigating such attacks are mentioned. Usage of IPsec, SEND, firewalls, IPS/IDS tend to be essential but they do not guarantee protection from malicious users if they are to apply without knowledge and proper configuration.

Appendix

Figure 14. Extension headers network topology.

Figure 15. Router R1 configuration.
Figure 16. Router R2 configuration.

```
interface FastEthernet1/0
  no ip address
duplex auto
speed auto
ipv6 address 2007:FF00:12FF:11:1/64
ipv6 enable

interface FastEthernet1/1
  no ip address
duplex auto
speed auto
ipv6 address 2007:FF00:12FF:12:1/64
ipv6 enable

interface GigabitEthernet2/0
  no ip address
negotiation auto
ipv6 address 2001:010:11:1/64
```

Figure 17. Router R3 configuration.

```
interface FastEthernet1/0
  no ip address
duplex auto
speed auto
ipv6 address 2007:FF00:12FF:21:1/64
ipv6 enable

interface FastEthernet1/1
  no ip address
shutdown
duplex auto
speed auto

interface GigabitEthernet2/0
  no ip address
negotiation auto
ipv6 address 2001:020:12:2/64
ipv6 enable
```

Figure 18. ICMPv6 network topology.
Figure 19. Router R1 configuration.

References


Network Penetration and testbed implementation for demonstrating penetrations using Metasploit Framework.

D. Petrinos¹, H. Katopodis²

¹ Dpt. of Automation Engineering and Electronics Engineering, "MSc in Networking and Data Communications", TEI of Piraeus, Greece, E-mail: dc-298@stef.teipir.gr

² Dpt. of Automation Engineering and Electronics Engineering, "MSc in Networking and Data Communications", TEI of Piraeus, Greece, E-mail: hkatopodis@yahoo.com

Abstract

This paper is to briefly analyze the penetration, refer to network and system vulnerability, security attacks and access compromises, and to implement a testbed for relative demonstrations. The testbed implementation is aiming to provide a step by step practical guide on how a student, in the lab of the university, can take control of some vulnerable virtual machines by using specific attack techniques and exploits provided by Metasploit Framework (MSF). The MSF is one of the single most useful auditing tools freely available to security professionals today.

1. Introduction

In recent years, the development and progress of our society has become dependent and is directly associated connected with Computer technology. Computer systems are used and are responsible for the most simple to the most complex human work. Yet one of the main features of the last two decades is the sharing and the storing of all enormous volume of information and data in a “world” network, the Internet, which is now an integral part of our everyday life and for many people the most important part of their lives. From this point of view, we realise that the security of information and data that moves from person to person – and why not from machine to man and vice versa – through computer networks, is a major issue.

The primary purpose of the computers’ security is to ensure that access to data and resources of computers becomes confidential only by those who have the right to do so, that the data remains intact and not altered by an unauthorized user and that the user always attested that indeed he is the one pretending to be. Undoubtedly there are many gaps in security systems that we use and constantly “discovered” new weaknesses. So the data resides in an environment constantly risks posed by unscrupulous trying to exploit security holes and attacks occur daily, without a lot of times the "victims" to notice them.

For this reason, the computer’s security must develop the necessary tools to ensure the above, to ensure that there are no risks that can cause some security holes, but attempts to control arbitrary actions and successful attacks on computer systems and
finally to guarantee and confirm the full system recovery in the event that any malicious actions cause changes on it.

2. Security in Information Systems and Networks

The current era is characterized by the very high growth of technology, the integration and introduction of the use of computers and information systems generally in all areas of human activity. The advantages resulting from this situation is equally significant with the risks arising from deliberate or unintentional human actions, like for example, destruction, alteration or unauthorised use of data and computational resources [1].

2.1. Why information systems are not secure?

A very classic and reasonable question that created in most people is why computers and information systems, in general, are not as secure as we need. Creators and functional systems administrators often avoid adding security attributes to them because it has meant creating problems to users. On the other hand, users circumvent security or override by choosing easy-to-use password and thus easily to discover. Almost always, software manufacturers distribute their products having preset out the features that will be installed, disabling security features. This is to avoid the problems to end users who do not have the skills and knowledge to understand and to properly regulate security features, which means that the vast majority of software installations have serious security problems.

In addition, software manufacturers focus their effort in adding features that will make their products more user-friendly and commercially, giving little importance to security. Consequently, since the development of secure information systems is a time-consuming process, the less secure products reach the market first and established.

For many years there is little diversity in the software market. The computer market is based on two basic operating systems, Windows and Unix. Accordingly, this means that there are small variants of these systems and the attackers have limited objectives to search and to find their vulnerabilities and their applications so to gain access to a large number of information systems.

2.2. Why computer networks are not secure?

The nature and the architecture of distributed systems increase the risks of intrusion and make it harder to implement and apply deterrent mechanisms. Some of the factors that characterize the difficulty of that output below [2].

Networks and distributed systems are dynamic and not static structures. Their composition is constantly changing because of technological progress, the expansion of the number of users and the extension of information needs and services offered. Also from geographical point of view networks’ coverage is constantly expanding.

The networks are structured with an abundance of natural resources and links - communication components. In many cases the physical access of the attacker is extremely simple, like linking to any exposed copper wire or in non-sheltered
concentrator, allocator. The use of cryptographic methods is more often non-economical efficient, due to the high computational effort required by the management of keys.

The current communicative structures interconnect heterogeneous networks and protocols. The universalization of security and cryptography protocols either is not possible due to the heterogeneity of communication protocols, either when it is possible to cause a high computing - communication burdens due to the necessary conversions of heterogeneous messaging protocols.

2.3. Attacking computer systems

Computer and network security is not based on a unique protection method, but uses a set of barriers that protect the data of each system in many different ways. Even if a measure fails to protect the system, the rest still function, so that it is sheltered from various attacks. Without security system installed, our systems are at risk of attack and use by unauthorized users, blocked network access, interruption of services, even possible theft and misuse of confidential business and personal information.

There are two ways to gain access to data and control the resources of a system, for a person who is not the owner of the computer or the computer administrator. The first is to have physical access to the information system and the second to connect to the system remotely.

2.4. Vulnerabilities – Exploits

But what is it that allows attackers to act and makes it possible to implement an attack? The answer to that question arises in the terms of “vulnerability” and “exploit”.

“Vulnerability” is the weakness that arises from the existence of a defect or problem, whose exploitation can lead to the violation of a system.

“Exploit” is the method by which the exploitation of a weakness and carried out an attack. From the moment you discovered vulnerability, an associated exploit is created which will be used in an attack. The vulnerabilities arise from defects that exist in various software that are due to bugs, from errors made in setting up systems, from software or design flaws from insufficient security measures.

At this point it is worth noting that because of the huge demand for progress in the field of technology, services and protocols that are used in networks and computers are evolving rapidly, as a result, with similar rhythm new vulnerabilities concerning their safety are revealed. A way to deal with this situation is by performing a “Penetration Test” in order to implement more efficient security possible.

3. Penetration Testing

The penetration testing is used by experienced users; to discover weaknesses that an information system has against attacks by malicious users. The huge range of attack tools and users willing to use them, are a big obstacle to security systems, resulting in
that penetration testing tools are the only guarantee that can someone looking to provide the best possible shielding of information systems. History has proven that any security system can be compromised, so the biggest opponent of each manager is time.

Penetration testing is a critical step in the development of any secure system as it not only stresses the operation, but the implementation and design of a system [3]. It is an authorized and scheduled act that separates a penetration tester from an attacker and has been widely adopted by the organization and institutions. What we are trying to achieve by executing a penetration test in a system is to gain knowledge and realize the vulnerabilities and how we can deal with them, before they become “tools” on the hands of an intruder / attacker for our system.

3.1. Penetration Testing Execution Standard (PTES) Phases

In general, Penetration Testing is a way in which the security evaluator can simulate the procedures an attacker would made to circumvent security controls and gain access to the system. However, because there are some differences in how they perceived the concept of penetration testing even in the area of security, the Penetration Testing Execution Standard (PTES) is redefining it by introducing some fundamental principles (phases) to carry out penetration tests [4]. These phases are:

“Pre-engagement Interactions”. It is the first phase where the safety assessor discusses with the customer about the terms and objectives of the evaluation. It is critical during this phase to be cleared the terms and objectives of the pentest.

“Intelligence Gathering”. At this stage, we collect as much information as possible about the company being evaluated, using social networking tools, Google hacking, etc. In this way, identify various intrusion points for the company, which may be either physically or electronically or human.

“Threat Modeling”. At this phase, any prior information gained, are used to identify all existing vulnerabilities of the target system. The most effective method of attack is determined and the evaluator acts as a rival and tries to use weaknesses like the attacker would do.

“Vulnerability Analysis”. At this point, you have to combine the information obtained from the previous phases and the results from scans of ports and vulnerabilities, to study and to understand what attack could be sustainable.

“Exploitation”. This phase focuses only on to succeed to gain access, by circumventing security restrictions.

“Post Exploitation”. This phase is a crucial point during the penetration test, as the evaluator distinguishes from the attacker. The evaluator or pentester, is now targeted to specific systems, infrastructure and crucial information or data to which the company gives more value and therefore wishes to protect.

“Reporting”. It is the most important point of penetration test, as created references as to what did the evaluator, how he did it, and most important, how the company can correct these weaknesses that were discovered.
3.2. Types of Penetration Testing

According to Kennedy D. et al. (2011) [5] a penetration tester, taking into account the previous seven categories of PTES, may carry out three different security assessment methods based on the perspective from which evaluates and interacts with the system. The “overt test” or otherwise “white box” test, is done with full knowledge of the organization, while “covert” (“black box”) is designed to mimic the actions of a sudden and unknown attacker. Both types have advantages and disadvantages. Also, there is one more which called “grey box” and has to do with the combination of the two above types of penetration tests. However, this requires an evaluator with limited knowledge of the inner system in order to choose the best way to evaluate overall safety.

The pentester needs some “penetration tools” to carry out the above security assessment methods. For that reason, there are many vulnerability monitoring tools available out there (penetration tools) that can identify with greater speed and effectiveness the different vulnerabilities. In this paper, we are using the Metasploit Framework (MSF), which is one of the single most useful auditing tools freely available to security professionals today, with a lot of exploits, built-in tools and vulnerabilities database.

4. Metasploit Framework (MSF)

The Metasploit Framework (MSF) is a famous security framework, in which the basis of the code is updated dozens of times daily by a main core of users, as well as from hundreds of submissions from members of the community. Originally developed and designed by H.D. Moore in Perl programming language. After the Metasploit 3.0 version was released in 2007, was adopted widely by the global security community and saw a large increase in the number of new users. In the fall of 2009, the Metasploit was acquired by Rapid7, which holds a leading position in the sector of scan vulnerabilities, which gave the opportunity to H.D. Moore to build a team that will apply itself fully in the development of the framework.

The MSF provides a complete infrastructure management and development of exploits, payloads, NOP (No OPeration) generators, protocols’ libraries, encoding routines while at the same time can cope with other tools to detect vulnerabilities in a computer system. It can be run at a command prompt by selecting the “msfcli” or the “msfconsole”. Alternatively the “msfweb” web server allows the user to have access to the MSF platform and its functions via a simple Web browser.

The Metasploit is not just a tool; it is an entire framework that provides the infrastructure needed to automate common but complex tasks. This enables the penetration tester to focus on unique or specialized aspects of penetration testing and to identify defects in the context of information systems security.

The Metasploit can be used in multiple ways. Allows easy integration of modules to increase potential security gaps, the payloads, the encoders and others, so as to establish and execute more advanced attacks. The MSF’s Architecture is shown in Figure 1 below.
“Framework Core”: The Framework Core of the platform consists of several subsystems, which are used for managing modules, sessions and processing outcomes and events. The kernel also provides the necessary links and interactive interfaces between the modules and plugins with all the rest of the MSF infrastructure.

“Framework Base Interfaces”. This component is located in the core of the platform and provides interfaces for facilitating interaction with the kernel. “MSF Console”. The console of the Metasploit Framework, is one of the most popular pieces of it, because it is one of the most integrated, supported and rich tools. Can be used for many things, like be used an exploit, to upload some auxiliary modules, to become massive exploitation of an entire network and others. Another interface is the “MSFCLI”. Unlike the msfconsole which provides an interactive way to use all of the user friendly functions, the priority of the msfcli is set for scripting and using other tools based on the console.

Another basic component of the MSF are the “Modules”. The Metasploit, as presented to the user, is composed of modules. A module (one unit or section), is a piece of software that can be used by the MSF. Sometimes you may need an “exploit module”, i.e. a piece of software, which performs an attack and is defined as a module which is using payloads. On other hand, an “auxiliary module”, which is defined as an exploit without payload, it can be used to scan or enumerate a system.

“Exploits”. They are written in Ruby and are the ones that trigger the overflows and exploit the vulnerabilities on the target server, while inject to it the selected payloads will execute code or perform useful actions.

“Payloads”. If the exploits are successful, there are many options for the actions to be taken to the target. The payloads are the pieces of code, which charge inside the target and are an integral part of the whole function of gaining access to the remote system.
4.1. Metasploit’s Basic Command Set

During the initialization of the msfconsole, all the “routine” checks for the right function of the console are carried out. If everything is as should be, we are going to see that the command prompt is changed from root@bt: to msf. In MSF’s command prompt we can input and the program will try to search any integer similar to what we have typed in order to run it. Typing “help”, a list of all available commands shows up, like those shown in Figure 2.

```
msf > help
Core Commands

Command     Description
---------    ----------------
?            Help menu
back         Move back from the current context
banner       Display an awesome metasploit banner
cd           Change the current working directory
color        Toggle color
connect      Communicate with a host
eixt          Exit the console
help         Help menu
info         Displays information about one or more module
irb          Drop into irb scripting mode
jobs         Displays and manages jobs
kill         Kill a job
load         Load a framework plugin
loadpath     Searches for and loads modules from a path
make         Save commands entered since start to a file
makefile     Pops the latest module off of the module stack and makes it active
previous     Sets the previously loaded module as the current module
push         Pushes the active or list of modules onto the module stack
quit         Exit the console
reload        Reloads all modules from all defined module paths
resource     Run the commands stored in a file
route         Route traffic through a session
```

Figure 2 Running “help” command in terminal.

By typing “show exploits”, a list of all available exploits shows up. The exploits are categorized by platform (Windows, Linux, ISS, Apache, etc.) and with a small description in what vulnerability refers to, its affection and date discovered.

The command “show payloads” lists all the available payloads. It also lists the name of payloads, the affection and a short description. In addition, we can use the “show payloads” command inside exploit’s command prompt, which results to list only the compatible payloads with that exploit.

If we want to recover information on certain exploit or payload, we use the command “info” followed by the name of the exploit or payload. i.e. info windows/shell_reverse_tcp.
Another command, which we are going to type most of the time in our scenarios, is the command "use". With the "use" command, we can choose which module we are going to use and as a result, the command prompt changes to where the module is.

5. **Penetration Testbed Setup and Scenario**

On a desktop computer, using Oracle's VM VirtualBox (Version 4.3.12 r93733), three separate virtual machines (VMs) were created. Oracle’s VM VirtualBox, is a virtualization software which allowed installing different operating systems on separate virtual machines on the same physical machine to simulate a cross platform environment. On the first virtual machine the distribution of BackTrack 5R3 Linux was installed, which acted as Pentester’s machine. The other two VMs were setup and configured to run one in Windows XP Service Pack 2 and the other a Linux installation of Ubuntu 9.04 Metasploitable, which were already set for the attacks. These two were selected because they are easier to exploit and quite vulnerable.

By using Metasploit Framework, integrated in BackTrack 5R3 Linux OS, we aim to safely demonstrate attacks on our lab virtual network, to uncover security issues and to assess and validate security risks in lab’s virtual machines for educational purposes and also to make students aware of the capabilities available to the public for free or at low cost.

The steps we follow in our testbed are: (a) “Mapping the Network”. We have to map our network and search target’s services, operating systems and anything that will be useful for our attack, (b) after finding vulnerabilities, open ports and running services, we choose which “exploit” we are going to use, (c) we configure our to exploit for use in specific IP address and remote port, (d) then choose the appropriate “payload” and configured it for the specific IP address and remote port, (e) finally, we use the “exploit” to release our attack.
5.1. Scenario: “Denial of Service” attack in Windows XP SP2 system

The “Denial Of Service” (DoS) attacks are mechanisms that have as their aim to make a computer system or a network unable to serve the authorized users. The attacks are designed to overload to a very large extent the target system by consuming memory and bandwidth. To achieve this, the attacker sends packets of data (fake login requests) to overly large pace so as to make it impossible to edit them from the target system, and in most cases be forced to restart (reboot). Of course, negative results are important when the attack takes place, not in a simple computer, but on servers.

For the DoS attack we are going to use a known Server Service vulnerability of the Windows. We use the "auxiliary ms06_063_trans", which operate some vulnerabilities in the Server Service of Windows that allow for denial of service and remote code execution in. In particular, these vulnerabilities (Server Service Denial of Service Vulnerability-CVE-2006-3942 and SMB Rename Vulnerability- CVE-2006-4696), exist in the Server service because of the way that it handles certain network messages. The attacker could exploit them by sending a specially designed message to a network computer that is running the Server service, and if the attack is successful, the attacker can gain full control of the system and to make it stop responding.

By typing the command "show options" in “auxiliary ms06_063_trans" command prompt we can see the necessary adjustments for the attack and with the command “set RHOST 192.168.3.11“ we define the Remote Host to IP address “192.168.3.11" as it is required by the “auxiliary”. Finally, the command “exploit" carried out the attack (Figure 4) and the target system displayed the blue screen and reboots (Figures 5).

![Figure 4](image-url)
Figure 5 System reboots and recovers after DoS attack and "blue screen".

6. Conclusion

The importance of computer security is the same as the importance of privacy. From the moment that almost all personal data of every modern man from the ID number and tax ID to his liking for music, friends and the products they buy are in electronic format and even in the "cloud" of the Internet, the above proposal seems self-evident.

From the first network worm until today the techniques used for the illegal access to computers have evolved and so have done the motives for the "shooting down" of the "relevant safeguards". At the same time, the market need for more and more features, combined with the requirement for lower prices makes the case of safe products to be far from reality.

A system is constantly exposed to many threats that exist on the network in which it participates. Malicious users trying to constantly identify and exploit weaknesses in systems with a view to gain control over it. These weaknesses can be either part of bad systems settings from their administrators or weaknesses of certain applications running on the system or even weaknesses in protocols used.

All the above are daily evolving, changing and presenting new features. For this reason an administrator can never be complacent but must constantly be vigilant and constant updating in order to be ready to face the challenges of accepting systems. In that way, the carrying out of a Penetration Test is mandatory.

The Metasploit Framework comes in handle for that reason as it is a multi-functional framework, rich in possibilities and options that constantly update and develop, since then creation of new technologies, programs and software, which is tested by the great community that is also immediately adds the new ways to attack and tests back in the
box. In this way, the framework does not ever get old, but rather always remains up to date and full of tools for each use. By using Metasploit Framework we aim to safely demonstrate attacks on our lab virtual network, to uncover security issues and to assess and validate security risks in lab’s virtual machines for educational purposes and also to make students aware of the capabilities available to the public for free or at low cost.

Acknowledgements

First and foremost I offer my sincerest gratitude to my supervisor, Dr Harilao Katopodi, who has supported me throughout my thesis with his patience and knowledge whilst allowing me the room to work in my own way after his initial determinative guidelines.

References

Networked Multi-Party Teleconferencing Services

A. Vlachou¹, A. Papadakis²

¹ Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: andriana0808@gmail.com
² Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: andreas.papadakis@gmail.com

Abstract

The last few years, the Voice over Internet Protocol-VoIP presents a rapid development and begins to be used more and more, both from big companies and from the wide public. This technology gives very cheap telephone services, with the quality to be better day by day and so is tending to replace the tradition telephony that all of us know. The purpose of this thesis is to describe in a simple way how this technology works and how can lead us in applications that ever we had imagine.

More specifically, in chapter 1, we are making an introduction of the history of traditional telephony how it works and the developments it had in the passage of time.

In chapter 2 is made an introduction to the world of VoIP. In the beginning becomes a brief historical overview about how the whole concept started. Thereafter is explaining the operation, the differences in relation to the traditional phone, as well as the future expectations that exist from the technological world for this.

In chapter 3, given a general image of the most important protocols that used in VoIP technology, SIP and H.323. Also are presented the basic principles of both protocols and at the same time becomes a comparative report on these.

Next in chapter 4 is analyzing the conference, what kinds of conference exist, how conference became important for companies and people, as also some of conference important uses.

Finally in chapter 5 an analysis is made on the application of Skype. How it works, what protocols and platforms use. How Skype change the lives of people around the world. And how useful can be in a company

1. Introduction

1.1. From the first telephone to VoIP

The PSTN network exists over a hundred years and all those years the philosophy remains the same. We could say that PSTN network is the most reliable system fixed by men and every time we lift the handset expect always to work taking it as a fact. The
impressive is that we can communicate with everyone, at any time, at any place of the world. Today is even easier to call someone, even if you don’t know his telephone number (using a telephone catalogue).

The key of success is the simplicity of all philosophy, two wires, a headset and a microphone. This is all we need for talking with someone all over the world.

2. **Section 1: Voice over IP**

- **What is VoIP.**

  VoIP technology uses the Internet Protocol - IP to broadcast voice signals in packet form above the internet, the VoIP can be achieved on any network that uses IP, such as Internet, Intranet and Local Area Networks – LANs. The voice signal in that technology is digitized, compressed, transformed into IP packets and subsequently emitted above the network IP. One of the main advantages of Internet telephony technology is the very small charge of calls

- **How VoIP works:**

  VoIP is a method for transforming the analogue audio signals (human voice) into digital information which may be transmitted in the Internet. This method, as is clear, has the potential to use a standard Internet connection and by the latest to make free telephone calls. All these in a combination with a variety of free programs that can be found on the internet for that purpose lead on in the widespread use of VoIP the next years, as set with this way bypassed the telephone companies as well as assistance to them entirely. So it is not excluded in the future this revolutionary technology to fully replace the existing telephone system.

- **VoIP Characteristics:**


- **Expectations for VoIP applications in the future:**

  Mobile phones, PDA and Wi-Fi phones, Cable and DSL modems, PBXs, Other hardware and software devices
3. Section 2: SIP and H.323 protocols

- **How SIP protocol works:** SIP is using addresses like those we use on e-mail because is the most common form of addressing through the internet. With a range of DNS tests as searching of service (SRV) is the server to which 'belongs' the user that makes the call. The advantage is that with this way it can easy be part of a website so by activating a link begins the call as is done in mail to: URL.

- **SIP Transactions:** After having found the terminal-transmitter the called user all requests are sending there. Every request with the responses that cause, make a SIP transaction. Requests can be sent even through TCP or through UDP protocol. If we will use a reliable protocol as TCP, then all messages from the same transaction, transferred through the same connection.

- **SIP Security:** 1) End to end encryption: Based on users keys. Every message is sending encrypted with the receiver key in order only he will be able to read it. 2) Hop-by-hop encryption: With this method we can encrypt the howl message. In that way (normally) the addresses of the users are talking, are not revealing in hackers.

- **H.323 Protocol:** H.323 covers both protected and unprotected connections. The data's and check information demand a protected transmission for avoiding the packet lost or receiving them in wrong order.

- **Architecturally Parts of H.323:** *Terminal, Gateway, Gatekeeper, Multipoint Control Unit – MCU*

4. Section 3: Conference

- **Types of conference:** 1) Room based systems: Room based systems allows in teams who are in a conference room to communicate with other teams of people. The cost of the room based video conferencing is high enough because of the demand for exclusive use in high end equipment. Basically those rooms are used by companies and satisfy communicate needs of their executives; sharing of data in real time, interactive communication of executives that otherwise is difficult to get in contact directly. 2) Desktop Videoconferencing: Desktop videoconferencing combines personal computing in combination with video and sound and also communication techniques in order to provide interaction in real time from a PC as well as combinations of interactive contacts between groups of people that are in rooms with computers. Those systems are very cheap comparing with room based
systems. They do not demand specific spaces either demanding facilities as regards the maintenance and regulation of these or guaranteeing the total reliability of data transfer.

- **Categories of Conferencing:** 1) **Video Conferencing:** In Video conferencing we have a conference procedure where participants share audio and visual messages in real time and use specifically network technologies. The advantage of this communication is of course the fact that the interlocutors have visual contact with each other and so is simulated in the best way the face to face communication. Naturally and conversed can hear each other or there is the ability to communicate through a friendly to the user interface for chat. There is also the possibility of exchanging the data used in the conference. 2) **Audio conferencing:** In Audio conferencing we have the communication-discussion among two or more individuals who using as a communication medium exclusively audio messages that are exchanged. That kind of communication can be done by either using very evolved and unaffordable audio communication systems such as the microphone or other devices either by using the telephone system that already exists. Regardless of the technology, the sound is the most important and older form of communication and it is the one who will give the features and transfer the opinions and the thoughts of interlocutors. 3) **Data Conferencing:** In Data conferencing the communication data are simple data's. They can have the form of a text, of graphics, of digital sound and digital video. The direct contact of the participants is not necessary. Data's that transferred among users using whiteboards or applications which allow in many computers to add, to remove or to processing archives. That’s a Data conferencing example without sound and video.

- **Uses of Conference:** 1) **Telemedicine:** The combination of new technologies and medical systems has opened new orisons and gave a more sophisticated dimension to the means, diagnosis and treating diseases. The applications that dealing with medical subjects and are combined with videoconferencing are called telemedicine and allowing the fast transfer of medical data that helps in better confrontation of medical incidents. The sources and their medical means of technologically advanced medical centres’ or hospitals allowing access to medical staff to get in touch with other doctors that are located in distant places and decide together for the deal of an incident. 2) **Distance Education:** The possibility of distance education gives the opportunity to people who wish to have access to knowledge to succeed without the necessary physical presence of the teacher or the learner. Also they can enrich the sources of knowledge since there is access to libraries or in places of education that are in a long distance from a point situated the person interested.

- **Video conference Vs Skype:** No one has even the smallest doubt that Skype made a lot for Video conferencing. The Skype transition from an audio service only to a video with audio allowed million people around the world to put video conference in their routine. Keeping in touch with your loved persons has never been easier and for free. Some other companies have overcome the success of Skype notably Apple with Facetime and Google with Google+ as well as a multitude of other chat and video applications. Out of the word of companies and clients, have spent and continue to invest millions of dollars each year for the enhancing
corporate video conferencing from dedicated video conference rooms, Telepresence suites to desktop and the emerging mobile video conferencing. One of the questions we often get asked is why not just uses Skype? Skype works with Skype. Unfortunately you cannot make a Skype call to a video conference room. Skype uses its own proprietary method of communication there have been some attempts to create video gateways from video conference rooms to Skype clients but all have had limited success maybe things will change on this front with the Microsoft acquisition of Skype although they may well tighten up further and only allow Skype to work with their own Lync offering. So, why you don’t replace your room system with a Skype embedded smart TV or a desktop PC? Rooms based video conference systems come at a price. They come at a price for very good reasons. They use high quality components to provide you with the best possible video conference experience. The table below shows the main differences in Skype in a meeting room versus dedicated hardware.

5. Section 4: Skype

- **Functions of Skype:** Skype in his simple edition gives free calls in the internet, either these are simple telephone calls either video calls. It is supports until nine, conference participants. The richest Skype edition called **Skype Pro** and it’s not completely free as the basic edition but provides same extra functions. Also somebody who enters in **Skype Credit** can buy with a low cost time for the charging services that Skype gives. One of them is the potential use and functions in mobile phones of NOKIA N series of his phones. In next lines, we will analyze the services that Skype gives for both services free and chargeable. So for free we have the **Skype to Skype** calls, the call transferring inside the network of Skype. Also for free provided and the video calls, the instant messaging, the group chat and the call forwarding into the Skype. In chargeable services, are included the calls to stable and mobile phones outside the network as also the receiving of calls. The use of voice mail is also chargeable as well as the promotion and diversion of calls to other networks. Also are charged the messages to mobile phones. But the cost of billable Services of Skype can reduced considerably if the user does not have the simple Skype edition, but the Skype Pro. Skype can also give solutions for professionals that are not simple users but they are interested in low cost communications. The Skype offers numerous functions in both simple and demanding users and takes up an ever growing percentage in IP telephony.

- **Skype Architecture:** Skype is a peer-to-peer VoIP client that developed after KaZaa in 2003. Supports whatever can operate through NATs and firewalls and also provides better sound quality from MSN and Yahoo IM applications even if his protocols and techniques are quite different from others. It uses a decentralized way in order to save his users information and hides end-to-end calls. Skype supports the instant messaging, as also the potential for teleconferencing and of course telephone calls from and to stable and mobile phones. Skype is an overlapping peer-to-peer network. There are two types of nodes in the network that are usual hosts and super nodes. For an example we can tell that a simple central computer is a Skype application that can allow calls and message sending. A super node is an end point in Skype network and can be anyone who has a public IP address. In
Skype network the login is made in the appropriate server, as the recognition of the user. The user ID and password are saved on this server and at the same time it is checked if the name of the user is unique in the space of Skype. Beyond this central server there is another server.

- **How Skype works in the progress of connection:** Skype is an overlapping peer-to-peer network of which each client has a set of nodes that called host cache. His nodes are simple and super nodes. Super nodes have a basic role and simple nodes are every node that has a public IP address with enough memory, bandwidth and a CPU with big memory. The main factor in the Skype network is the node for the login of the users in which into him are stored information that have to do with usernames the lists that they have their contacts and the password of each user in order to connect with the server. The procedure for client login is complicated and is analyzed in the next lines in two basic steps: the step that the client installs a connection with the super node and the step where the client connects and been recognized by Skype’s login server. With more details, in first step in order to achieve the connection with the super node reads the IP address and the number of the gate from the archive of the host cache. Then is trying to connect in the super node through UDP, TCP in a specific gate. In the case that is not valid the entrance in the host cache there are 7 addresses for the super node that is located in the hard of the code. After he passes the first step of login, the client asks from the super node the address for the login server. After that is linked to TCP server and attempts of identifying if he can or not be connected with him namely whether exist or not a firewall and if yes then passes the messages for the login through the super node. After that recovers the list of his contacts from the login server. Regarding to identify a user in Skype is used the Global Index algorithm that guarantees the identification of users that are in the internet the past 72 hours.

The process for locating the user follows the following steps. The client asks the super node for a specific user. The super user from his side, must answer with 4 addresses which and is looking for and the client makes questions in super node over the UDP and continues to ask until there is a success. After this and in case that was unsuccessful the research, then the login server been used like the one that will give the answer instead of the super node. Also the client can use the search algorithm and asks from the super node to make the research and to return the results. After the research to identify of the user has been completed successfully, we are stepping to the next phase of the program that regards the establishment of a call. The three basic spots that constitute this part are the signalling of the call over TCP, the streaming of both voice and video and the codec’s for the voice streaming.

The first basic spot for the call establishment is the call signalling over TCP straight and directly between the called and the user that makes the call or when there is NAT / firewall that are blocked with that way the direct communication to take the super node.

The second spot are the voice and video streaming which happens above UDP directly between the participants. In the case that one of them is behind of a NAT, then a margin in the UDP enables the direct communication. But the voice and video streaming can also be performed above the TCP after being sent from the super node when a firewall blocks the traffic flow of UDP.
The third spot that defines the call establishment are the codec's which are used for voice streaming. Is supported that used wideband codec's, iLBC, iSAC, iPCM. The frequency is between 50-8000 Hz while the use of bandwidth is around 5-5.5 kB / s.

6. Conclusion

The IP telephony through data networks (VoIP) is a relatively new technology which tends to abolish the traditional telephony. In the last years, with the help of development-improvement of IP networks and the spectacular increase broadband connections for internet access (technologies of ADSL, VDSL). VoIP is now a mature technology and considers able to replace the traditional telephony. Moreover, it is no coincidence that the alternative providers of telecommunications already use VoIP technologies to transfer phone calls on the inner proprietary network of their trunks. In addition, more and more businesses, perceive the benefits that can be gained from using the VoIP service, and for this they have replaced the antiquated telephone network with an internal IP network that can be used in parallel for data and voice.

In the recent future, VoIP telephony will totally replays the traditional telephony. Will provide Subscribers only some form of broadband connection to access the Internet which will be used in conjunction for data transfer but also and telephone calls.

The revolution of VoIP protocol came with the application of Skype. An applications with much better qualifications from VoIP, such voice quality, ability to traverse the NAT and firewalls, encrypted media channel, ability to scale up to handle large-scale connection-oriented real-time services such as voice, etc. However Skype's success, became because Skype is based on a P2P overlay networks. It makes use of several great technologies and integrates them very skillfully.

With the passing of years we have seen that technology evolving with tremendously rapid rhythms and continually making their appearance new and more reliable application that make communication easier and more accessible to all sides of the earth.

Acknowledgements

I would like to thank my parents for the supporting all this years.

References


Planning and deployment of a roaming capable secure Wi-Fi network

I. Spanos\textsuperscript{1}, H. Katopodis\textsuperscript{2}

\textsuperscript{1} Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: spinspan@gmail.com

\textsuperscript{2} Dpt. of Automation Engineering and Electronics Engineering, “MSc in Networking and Data Communications”, TEI of Piraeus, Greece, E-mail: hkatopodis@yahoo.com

Abstract

Wi-Fi is cheap, easy to deploy, scalable, portable and ubiquitous. This paper attempts to describe the challenges this wide adoption creates, its performance and security aspects, the challenge of high density client environments and their need for roaming, and how to plan and deploy a solution using the latest developments in the field.

1. Introduction

Despite the existence of emerging and promising technologies such as LTE an already mature technology such as Wi-Fi is chosen. The reason? Its explosion of use. In any case the growth of Wi-Fi is mainly due to the fact that it is a technology addressed to the masses. It gives access to the Internet, it is cheap, easy to deploy, scalable, portable (unlike WiMAX), and ubiquitous. It is in our homes, at hotels, at cafes, at restaurants, in stores, at squares, at airports even in airplanes. Even Google is sending Wi-Fi enabled balloons in the stratosphere (Project loon). However there is no lack of safety and capacity issues.

ITU reports that in 2013 more than 2.7 billion people accessed the internet, which is almost half of the world’s population, and the penetration of the smartphone market must be a good reason for that. According to Cisco, during the same year mobile devices outnumbered the people on earth. According to Aaron Smith from Pew Research 44\% of smartphone owners have slept with their cell phone next to their bed to ensure they would not miss any messages during the night, while IDC reports that 79\% of smartphones owners check their device for new emails or social networks feeds within the first 15 minutes of waking up. In a New York Times survey 75\% of Americans responded that Wi-Fi abstinence for a week is more unpleasant than coffee drinking abstinence. More than 64\% of hotels nowadays offer free wireless access, as 94\% of all visitors consider the existence of Wi-Fi an important amenity, while 38\% of them cancel the reservation if there is no free access to Wi-Fi. Also mobile network operators consider Wi-Fi technology as a great commercial growth opportunity, rather than a competitor. The French mobile operator FREE provides contract plans in conjunction with free Wi-Fi access.

Retailers are positive to integrating Wi-Fi networks with their stores’ infrastructure, as they may offer various services increasing their profit and improving their business
profile. Consider consumers who use a smartphone in-store or a tablet and the first page they can read is a splash screen with the retailer's message.

Corporations can also benefit from the use of Wi-Fi technology, since it is very flexible, cheap (license free) and easy to expand. In many cases, wiring can be difficult or impossible, and the installation of new cables can prove costly or time consuming. In another instance of a business need to immediately connect new workstations to the corporate network and there isn’t enough wired resources, Wi-Fi could be once again a good solution. The demand for higher speeds is reflected in the leaps that have been made since the release of the basic 802.11 protocol in 1997 specifying data rates up to 2Mbps. Wi-Fi growth required the design of higher capacity and more secure wireless networks, so in this thesis will examine the technologies based on the IEEE 802.11 standard and the safety issues that threaten users of wireless networks. Reference will be made to the behaviour of electromagnetic waves and radio frequency propagation, as well as the types of antennas used in wireless LANs and the additional information needed when considering the design of wireless networks. We will refer to topologies of wireless networks and roaming issues. A wireless network will be deployed in camp using the theory that we consider, and we will describe some of the services that can be provided in a wireless network and attempt installation on the pilot network. Finally, we will evaluate the network performance, and discuss the issues.

2. Wireless transmission

Radio wave penetration is the propagation through a significant mass. A radio wave is an electromagnetic wave that is transmitted via an antenna [1]. Frequency and amplitude are the two main components of radio waves. In order to establish wireless communication between two or more devices they must be tuned in a specific frequency. Regarding sinusoidal waves, frequency is the number of times of a periodic cycle per second and its unit is hertz (Hz). The frequency (f) is reverse related to the wavelength and is given as:

$$\lambda = \frac{c}{f}$$

Where \(\lambda\) express the wavelength in meters, and \(c\) the speed of light in vacuum (300.000.000 m/sec)

3. 802.11 and successors

802.11 is the wireless local networks standard, which was originally implemented by an IEEE LAN/WAN standards committee in 1997. According to 802.11 specifications the possible data rates were 1 Mbps or 2 Mbps, and the radio spectrum that could be used is the 2.4GHz band. Two main characteristics increased the speed and reliability of wireless networks: the OFDM modulation (Orthogonal Frequency Division Multiplexing) in conjunction with the MIMO technology (Multiple Input Multiple Output). OFDM is interference and multipath resistive allowing higher data rates in neighborhood channels. In OFDM modulation the channel consists of multiple subcarriers in contrast to other modulations consisting of one main frequency carrier [2]. MIMO is compared to a serial to parallel adapter, as it divides the outgoing traffic in multiple data streams (clock related) which are transmitted by particular radios and antennas, and vice versa
[3]. For instance a 2x2 MIMO radio system consists of two radios and two antennas, which are able to transmit and receive simultaneously two data streams in parallel.

<table>
<thead>
<tr>
<th></th>
<th>802.11</th>
<th>802.11b</th>
<th>802.11a</th>
<th>802.11g</th>
<th>802.11n</th>
<th>802.11ac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Data rates per stream</td>
<td>2 Mbps</td>
<td>11 Mbps</td>
<td>54 Mbps</td>
<td>54 Mbps</td>
<td>150 Mbps</td>
<td>866.7 Mbps</td>
</tr>
<tr>
<td># of streams (MIMO related)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Operating bands</td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
<td>5 GHz</td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
<td>5 GHz</td>
</tr>
<tr>
<td>Channel bandwidth</td>
<td>22 MHz</td>
<td>22 MHz</td>
<td>20 MHz</td>
<td>20 MHz</td>
<td>20 MHz</td>
<td>40 MHz 80 MHz 160 MHz</td>
</tr>
<tr>
<td>Modulation</td>
<td>DSSS, FHSS</td>
<td>DSSS</td>
<td>OFDM</td>
<td>OFDM, DSSS</td>
<td>OFDM</td>
<td>OFDM</td>
</tr>
</tbody>
</table>

The main 802.11 protocols.

4. Channelization

Although in fact the effect of these jammers is limited to a few meters from the emission point, it cannot be overlooked. Technically usable as they do not overlap each other, and these are channels 1, 6 and 11. The 802.11a, 802.11g and 802.11n amendments implemented 20MHz space channels.

In order to expand the radio coverage of an area the three non-overlapping frequencies may be used and reused by placing the radio systems in different distant locations,
making spatial divisions of virtual cells. Taking advantage of the frequency reusing concept the network capacity is increased as the interference is decreased.

A frequency reuse concept with three non-overlapping channels.

5. **Wireless LANs modes**

There are three different types of Service Set with which WLANs are organized, the Basic Service Set (BSS), the Extended Service Set (ESS), and the Independent Service Set (ISS).

The BSS consists of a wireless Access Point (AP) directly connected to the wired network and one or more wireless stations, and its operation is referred to as Infrastructure Mode (IM). In IM mode the stations are required to be connected to the AP in order to gain access to the network. All stations must be in proper range in order to communicate with the AP. The closer to the AP a station is the stronger the signal becomes, and as a result faster data rate is achieved. The BSS has a unique SSID, which is the name of the BSS and stands for Service Set Identifier.

BSS – Infrastructure mode
The essential definition of the ESS is that it contains two or more BSSs sharing a common distribution system such as wired network.

Also the ESS contains two or more cells, which may or may not overlap.

6. Roaming

In general terms roaming is the process of maintaining the connectivity to the distribution service network by moving from the range of one BSS cell to another of the same ESS. In standard 802.11 based networks the roaming decisions depend on the wireless station. In fact there is measurable transition time because of the re-association and perhaps the re-authentication processes.

The main problem with legacy 802.11 devices is that they have the sole responsibility for the roaming behavior. 802.11 was not designed for roaming use, neither catered to
any Quality of Service concepts, thus the transition times are significantly greater than the mobile equivalent. In addition the Authentication process times are not fast enough. Improvements are going to be made by implementing the 802.11i, 802.11k, and 802.11r standards. The 802.11i standard promises among others to provide fast Authentication with the Opportunistic Key Caching (OKC) feature, the 802.11k will allow fast BSS transition (handoff) and finally 802.11r will use the Radio Resource Measurements of the WLANs feature allowing the stations to maintain association with multiple APs and providing them with prediction capabilities about the radio performance in order for them to make faster and more reliable decisions of when and to where to roam.

7. **Authentication and Association**

Authentication is the process of the verification of the identity of the wireless station by the AP, and it happens after the station has located the preferred network. In order for a station to have access to a specific AP initially it must be authenticated. After a successful authentication the association process follows, and if it is successful too it will give the wireless station the permission to exchange data with the AP.

In standard 802.11 networks both the Authentication and Association processes begin from scratch every time the wireless station roams from one BSS to another within the same ESS. That increases the transition time, thus the 802.11r amendment, which allows the pre-authentication of the wireless station by the next associated AP resulting in a smoother or even seamless roaming perception.
8. **Authentication types**

Two main methods of Authentication process are specified by the IEEE [4], the Open System and Shared key, while the 802.1X with EAP comes to supplement the wireless network security options.

The Open System is the default authentication method of the stations by the APs and actually uses no authentication mechanisms such as usernames or passwords or anything else, there is no security policy. However data encryption (i.e. WEP) process might take place but only after the authentication and association have finished successfully.

In the Shared Key authentication method strings of text or numbers are exchanged representing a passphrase (password key). In order for a wireless station to gain access to an AP both must be pre-configured to set the same encryption key, known as WEP key (Wireless Equivalent Privacy). The AP sends to the wireless station which wants to be authenticated a challenge phrase of random characters. The station encrypts that phrase with the WEP key and sends it back to the AP. The AP will decrypt the encrypted challenge phrase using its WEP key and compare it with that was previously sent. There are security issues by using Shared Key authentications as the challenge phrase is broadcasted in clear text, so it is easy for an intruder to capture both the challenge phrase and some encrypted data (some thousands frames) and crack the WEP key.
The 802.1X in conjunction with the EAP (Extensible Authentication Protocol) authenticates the user versus the station, and that is done in conjunction with a RADIUS server (Remote Authentication Dial In User Service) [5] [6] [7].

The RADIUS server here acts somehow as a gatekeeper, as the AP forwards the requests of the wireless station to the RADIUS server and then it responds to the wireless station passing the challenge through the AP. The user credentials may be stored perhaps in a Microsoft Active Directory, in a LDAP server, in a MySQL data base, or in a custom data base such as the Mikrotik’s UserMan implementation.

When the wireless station makes an Authentication request, the AP responds with an EAP identity request. The EAP is called extensible because it may use different type of authentication protocols, so for example Digital Certificates (in example a Smart Card).
or Subscriber Identity Module (the SIM card used in GSM mobile) could be used. After the user verification the RADIUS server suggests to the AP to grant access to the station.

9. Planning

The project of this thesis consists of the planning and deployment of a secure Wi-Fi based wireless network, which will cover a camping. The budget should not exceed EUR 4,000.

The camping area.

The settlement camping area is approximately 25 acres, and it is mainly covered by trees. Furthermore, because of the Greek marketplace penetration, systems operating in the 5 GHz band are extremely few, therefore the 2.4 GHz band was selected to operating the APs. Consideration was given that the antennas should not be installed at a height greater than that of the pine foliage.

For testing purposes one radio system was setup on selected fixed locations, and measurements of signal strength were taken by the use of a laptop in conjunction with an external wireless adapter. The measuring adapter is the dual band ALFA AWUS051NH that works on 802.11a/b/g/n modes, and the test AP consists of the dual band Mikrotik Groove A-52HPn and a 10 db omnidirectional antenna. 300 concurrent wireless devices of any type might be connected to the network, if both the visitors of guests and the camping staff are aggregated.

The budget allowed implementing only three hotspots consisting of two Access Points with an antenna for each AP, and their bridging radio systems. In conjunction with performing of the live walk-through survey a predictive design of the coverage map was implemented by using the professional tool of RadioCoverage.com, which drew the predicted final heat map.
The tool needs the coordination of the installed radio systems and their full characteristics (antenna properties, cable losses, power of the emitted radiation, frequency, etc.). It is possible to configure the azimuth and the antenna tilt to in order to achieve the desired coverage, making as much tries as needed.

![Characteristics configuration in the Radiocoverage.com tool.](image)

<table>
<thead>
<tr>
<th>APs location</th>
<th>Latitude</th>
<th>Longitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entrance</td>
<td>38.062316°</td>
<td>23.994224°</td>
</tr>
<tr>
<td>Water tower</td>
<td>38.061908°</td>
<td>23.995876°</td>
</tr>
<tr>
<td>Restaurant</td>
<td>38.063339°</td>
<td>23.995897°</td>
</tr>
</tbody>
</table>

The location of the APs
The entrance of the camping

The old water tower
The line of sight between the water tower and the restaurant

The predicted radio coverage is as follows:
The final predicted radio coverage is illustrated with a red layer.

The colour does not correspond to the signal strength.

10. CAPsMAN centralized management approach

CAPsMAN is a proprietary feature of Mikrotik’s RouterOS and stands for Controlled AP System Manager. A CAPsMAN controls the Access Points within the network, also can manage the authentication of the end clients. It is able to make data process (if it is necessary and that is the default configuration), so all incoming and outgoing data traffic is processed before routed. CAPsMAN is built around two main entities in a system: at least one CAP (Controlled Access Point) and one System Manager (CAPsMAN). Within the campsite network are installed six CAPs communicating with the main (CAP1, CAP2, CAP3, CAP4, CAP5 and CAP6). These CAPs are managed just from the main router which acts as the CAPsMAN and all the wireless interfaces may be controlled in centralized logic (wireless protocol, frequency band, security profiles etc.).
The CAPs are dedicated to provide only the necessary connectivity and encryption to the end wireless stations saving CPU load of their motherboard and the CAPsMAN will shoulder the authentication and the traffic process. The CAPs are fixed to selected sites within the campsite in significant distance from the main router.

One Routerboard RB951 will act the role of the CAPsMAN. This devices is not expandable to wireless interfaces but is equipped with five Gigabit Ethernet ports.

11. The implementation

It follows the proposed logical network map.
12. FreeRadius, Daloradius and MySQL

FreeRadius in conjunction with both Daloradius and MySQL will be implemented in order for our network to get AAA capabilities. All three packages will be installed in the same computer that will be connected to the Ethernet 3 port of the CAPsMAN. CAPsMAN will act as the Radius client, FreeRadius will be the RADIUS server, MySQL will store the user credentials, and the Daloradius will be the web front-end to the FreeRadius in order to create Users.

13. pfSense

pfSense is an open source firewall distribution based on FreeBSD. PF stands for packet filtering, and includes many features such as load balancing, firewalls, traffic shaping, packet sniffing, dynamic DNS, VPN, captive portal and many more. Many plugin applications which may be installed at a later time have been developed to enhance the performance of pfSense. Intrusion detection such as Snort and web proxy Squid are some of these plugin applications.

14. Post-deployment site survey

Post-deployment site survey performed by using the TamoGraph Site Survey software. Results are as shown below. The red color areas performed the weakest signal strength (almost -85 dBm), while the green color areas performed the strongest signal (almost -45 dBm)
15. Network performance

The average throughput was determined at 7.35 Mbps. At the time almost 150 people were in the camping. The measurements were made by using the network performance tool iperf (https://iperf.fr).

16. Roaming performance

The average transition time of roaming performance indicated at 250 ms.

17. Conclusion

The advantage of site survey pre-deployment method is that it visualizes the real performance of the network. But in contrast to the use of software based propagation prediction tools it is time consuming and knowledge demanding. The software planning tools are cost effective and are highly recommended especially in large deployments, though the provided accuracy is not guaranteed under every environment circumstance.

Wide use of secure authentication methods such as 802.1X in conjunction with EAP is a must solution. The vulnerabilities of the past have taught us that strong encryption is the integral part of the future telecommunications.
The use of multiple radio cells in conjunction with the high demanding of secure access are the common foe against the compatibility of roaming capabilities with the today's 802.11 standards. New roaming friendly standards such as 802.11r have to implement in order to offer better quality services to the users. The use of the 5 GHz band or the extension of the 2.4 GHz band in conjunction with the exclusive use of high coding schemes such these of 802.11n or 802.11 ac could support higher density wireless networks. The use of Multiple Access schemes like TDMA or OFDM should consider the network planners.

The pre-deployment, the post-deployment and the troubleshooting must be performed in conjunction with state-of-the-art tools such as spectrum analyzers and protocol analyzers. Spectrum analyzers offer incredibly fast first view of the actual condition and help the network planners to prepare their next action. The site survey tools offer a friendly reading reports to the end non-professional user who are able to read map or floor plans with color code radio covered areas. Although the real problems can be revealed only by use of a protocol analyzer can sniff the wireless data frames.

18. Acknowledgment

This project gave me the opportunity to study my favorite subject, wireless communications. I would like to thank my supervisor, Dr. Harris Katopodis for providing trust and guidance to complete this project. I would like to thank the TEI of Piraeus, the Kington University and my professors who have contributed to my Master in Networking and Digital Communications. It was a pleasant and creative period. Last but not the least I would like to thank my wife Vicky and our daughters Olivia and Yvonne who have deprived of my attention and presence for a long-time.

19. References