Al-Khwarizmi Engineering Journal

Al-Khwarizmi Engineering Journal, Vol. 8, No. 1, PP 1 - 10 (2012)

WLAN Integrated with GPRS Network Securely

Mohammed A. Abdalla* Khalifa A. Salim**
Zinah Jaafar Mohammed ***

**Department of Information and Communication Engineering/ College of Information Engineering/ University of Al-Nahrain*
***Department of Information and Communication Engineering /Al-Khawarizmi College of Engineering / University of Baghdad*
****Department o Computer Engineering and Information Technology/University of Technology*
* Email: mohammedalmushdany@yahoo.com
** Email: khalifaabboud@yahoo.com
*** Email: Zinahameen83@yahoo.com

(Received 24 March 2011; accepted 18 October 2011)

Abstract

In this paper a WLAN network that accesses the Internet through a GPRS network was implemented and tested. The proposed network is managed by the Linux based server. Because of the limited facilities of GPRS such as dynamic IP addressing besides to its limited bandwidth a number of techniques are implemented to overcome these limitations.

Dynamic Host Configuration Protocol (DHCP) server was added to provide a single central control for all TCP/IP resources. Squid Proxy was added to provide caching of the redundant accessed Web content to reduce the Internet bandwidth usage and speeding up the client's download time. Network Address Translation (NAT) service was configured to share one IP address among several different systems. In order to accomplish a secure channel to exchange data between two network devices, the Secure Shell (SSH) protocol was added.

The first test shows that the data transfer rate at different time intervals of the day found to be an average of 10.95 Kbps for uploading and 13.7 Kbps for downloading and the second test shows that the network performance improved when squid proxy cache was used. The data rate found to be 143.3 Kbps average for uploading rate and 376.6 Kbps average for downloading rate.

Keywords: *GPRS, server, openVPN, security*.

1. Introduction

Wireless Local Area Networks WLANs offer high data rate Internet protocol network connectivity using the Industrial, Scientific and Medical (ISM) band which is license free radio frequencies, but problems of limited coverage area still exist. WLAN networks are mainly an indoor environment for low mobility and high speed applications. The bit rate of IEEE 802.11b standard can achieve 11 Mbps, while the 802.11g standard can achieve data rate up to 54 Mbps [1].

Cellular operators are already capable of providing wide coverage area with cellular technologies, with the same wide spread coverage as voice services. Besides that, cellular operators have a large customer base which put them in a good position to complement the service offering by WLAN.

General Packet Radio Service (GPRS) is a cellular operator service that supports increased demand for Internet services over a wide area besides the mobility needed. GPRS is a wide area data solution, but it is not able to support the high data rate required for various applications due to its limited bandwidth.

In this work, an integrated WLAN combined with GPRS network system was implemented and tested to access the internet based on GPRS as a service provider. The rest of the paper is organized as follows. Section 2 describes the GPRS network architecture. In section 3 both

server implementation and client configuration of the proposed system architecture discussed. Section 4 deals with network assessment and finally section 5 lists some concluding remakes.

2. GPRS Network Architecture

GPRS is a packet-based data bearer service for wireless communication data transfer that is delivered as a network overlay for GSM, CDMA and TDMA networks. Theoretical maximum speed of GPRS is up to 171.2 kbps [2].

Packet switching means that data is split into packets which are transmitted separately and then reassembled at the receiving end. However, packet switching means there is no dedicated circuit assigned to the GPRS mobile phone [3]. A physical channel is established dynamically, only when data is being transferred. Once the data has been sent, the resource (a timeslot on the air interface) can be re-allocated to other users for more efficient use of the network.

GPRS attempts to reuse the existing GSM network elements as much as possible, but in order to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols that handle packet traffic are required. The existing GSM compatible devices do not handle enhanced interfaces, and do not have the ability to packetize traffic directly. Either voice or data traffic is originated at the subscriber terminal, which would be transported over the air interface to the Base Transceiver Station (BTS), and from the BTS to the Base Switching Center (BSC), in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated to voice which is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the Serving GPRS Support Node (SGSN), via the Packet Control Unit (PCU) over a frame relay interface.

The SGSN can be viewed as a packet switched MSC that delivers packets to mobile stations within its service area. SGSNs send queries to the Home Location Register (HLR) to obtain profile data of GPRS subscribers. SGSNs detect new GPRS mobile stations in a given service area, process registration of new mobile subscribers, and keep a record of their location inside a given area [4].

The elements of a GSM/GPRS network are shown in Figure (1), where the special GPRS communication interfaces are indicated.

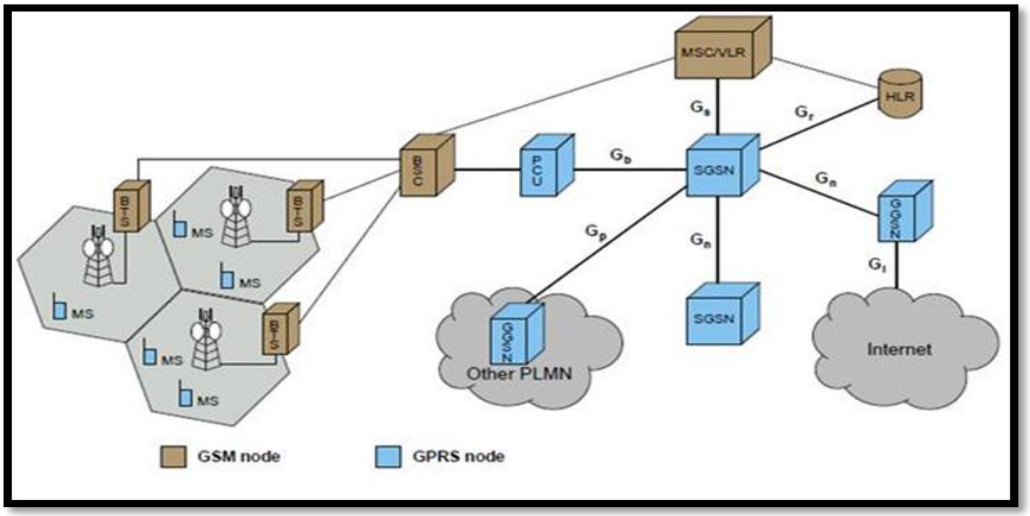

Fig. 1.GPRS Network Architecture [5].

3. Proposed system Architecture[6]

Figure (2) shows the network components which consists of a switch used to connect the private network under test with its private range of IP addresses defined by the server and one access point attached to the switch in order to enable client's hosts attending the network through Wi-Fi. To set a GPRS connection for the network a mobile station is used and configured by the server, hence establishing Internet connection via GPRS by using the mobile device as modem.

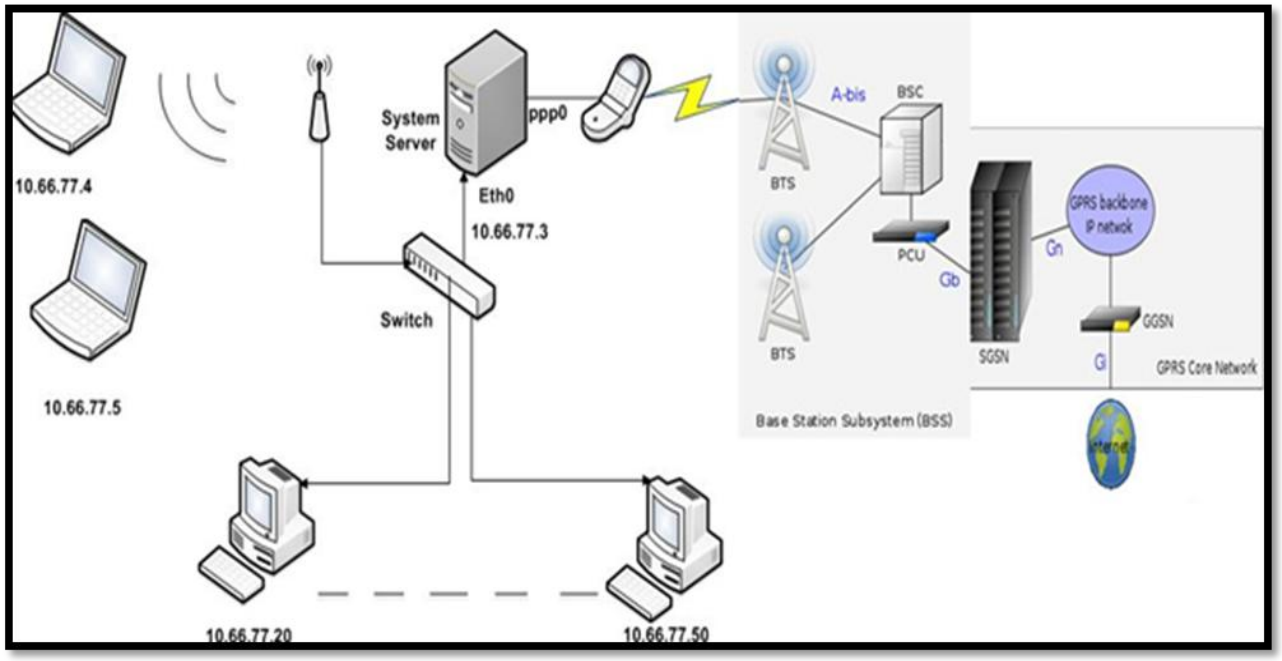

Fig. 2.Actual Implemented and Tested Network.

The system implementation is divided into two steps:

3.1. Server Implementation

GPRS connection is established by using mobile device connected to the server via a USB cable or Bluetooth as shown in Figure (3).

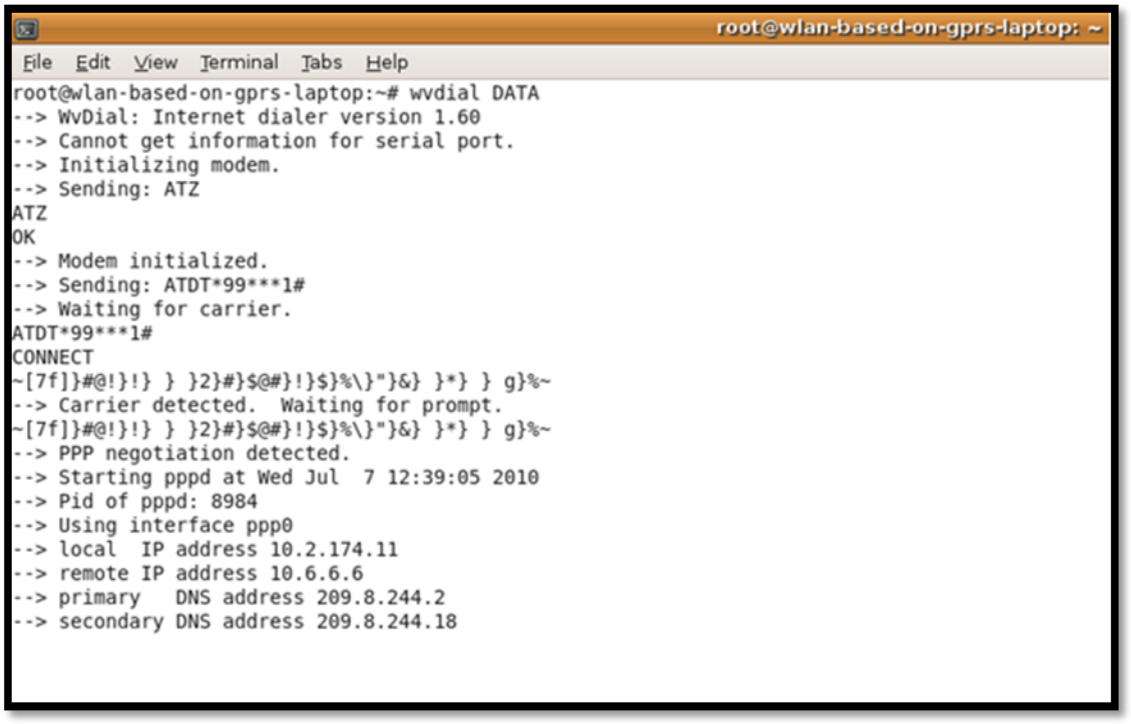

Fig. 3.Establishing Internet Connection.

The network is managed by the Ubuntu Linux server. The server is implemented by configuring the DHCP server. It is used to configure all client machines in exactly the same way by configuring them to use the DHCP server. It is also much more reliable than manual TCP/IP management, because the DHCP server is designed to manage its IP pool and the lease periods so that never get two hosts using the same IP address at the same time.

DHCP server lease the address to the client for a specified time, a test to the server was done as shown in Figure (4).

```
lease 10.66.77.4 {
  starts 3 2010/10/13 14:46:38;
  ends 4 2010/10/14 14:46:38;
  cltt 3 2010/10/13 14:46:38;
  binding state active;
  next binding state free;
  hardware ethernet 00:23:8b:4f:40:8d;
  uid "\001\000#\2130@\215";
  client-hostname "Zeyna-PC";
}
```

Fig. 4.DHCP Server Leases File.

One of the client IP lease that was offered by DHCP server to a client with the host name Zeyna-PC. This test confirmed that DHCP service was configured correctly.

Squid proxy is used for authorization and controlling the Web pages filtering. It provides a control point for restricting which of external Web sites can be reached. Authorization is needed to prevent unauthorized users to access the Internet especially through the access point. Besides that squid proxy is mainly used to provide Web page caching. It caches the commonly accessed Web and FTP content locally, thereby reducing the Internet bandwidth usage and speeding up client's download time.

Squid was checked by viewing the access.log file which provides a valuable source of information about Squid workloads and performance. The logs record contains not only access information, but also system configuration errors and resource consumption (such as memory, disk space). As shown in Figure (5).

```
1288112022.531   3535 10.66.77.4 TCP_MISS/200 10930 GET http://www.4shared.com/ second_user DIRECT/72.233.72.139 text/html
1288112023.152    127 10.66.77.4 TCP_REFRESH_HIT/304 308 GET http://www.statcounter.com/counter/counter.js second_user DIRECT/
93.188.130.42 -
1288112023.288     98 10.66.77.4 TCP_REFRESH_HIT/304 346 GET http://www.google-analytics.com/ga.js second_user DIRECT/74.125.7
7.101 -
1288112024.573   1855 10.66.77.4 TCP_REFRESH_MISS/200 11036 GET http://www.4shared.com/images/all1.png second_user DIRECT/72.2
33.72.156 image/png
```

Fig. 5.Access.Log File.

In order to effectively configure the Linux server to operate as router, packet forwarding is enabled, in order to forward the incoming packets on one interface to another based on the packets destination address. Each interface must be configured with a unique IP address. If two networks use separate media (Ethernet, PPP, other), packets are automatically transformed to match the other medium's specification.

IP tables rules are added to force all the TCP traffic inside the private network with the destination port 80 to be redirected to port 3128, squid's specified port of the server besides enabling NAT/IP masquerading in order to activate Internet sharing among the private network computers.

To test if NAT works properly would be on the clients' side, as the clients can access the Internet provided by the server. This means that the added rules worked correctly.

Open SSH is an open source implementation of the SSH protocol suite that provides encrypted communication sessions over a computer network, enabling remotely controlling a

computer or transferring files between computers securely. Traditional tools used to accomplish these functions are insecure and transmit the user's password in clear text when used.

For security consideration, Open SSH would listen for the incoming TCP connection on port 8381 instead of its default TCP port 22. Open SSH server is configured to enable public key authentication so that the generated keys could be either DES or RSA.

In order to access the Open SSH server remotely besides its local access, both the Open SSH server and clients should get IP address from the public range of IP addressing, therefore and for testing purposes Hamachi software is suggested.

Hamachi is a zero configuration VPN application capable of establishing direct links between computers that are behind NAT firewalls, in other words, it establishes a connection over the Internet that emulates the connection that would exist if the computers were connected over a local area network [7].

Hamachi is a centrally managed VPN system, consisting of the server cluster managed by the vendor of the system and the client software, which is installed on end user computers. Client software adds a virtual network interface to a computer each client establishes and maintains a control connection to the server [7].

In order to test Hamachi, and check if it was installed, configured and would work properly at the server host, ifconfig command was used which displays information on all network interfaces configured in the Linux kernel information such as an interface, netmask and the IP address.

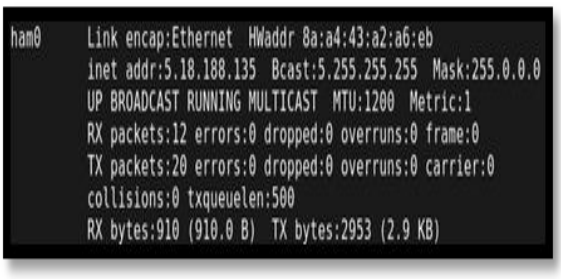

Fig. 6. Hamachi Virtual Network Interface.

As shown in Figure (6), ham0 was created which assigned a class A public IP address that is 5.18.188.135 with network mask 255.0.0.0.

Open SSH test was done by executing the command netstat, which returns the network information. This command was issued to check if the server is listening for incoming connections as shown in Figure (7) the SSH server port was listening and working on 8381 port with process ID 5493.

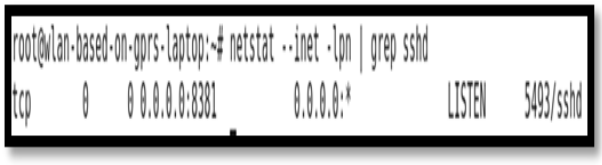

Fig. 7.Checking SSH Server.

3.2. Client Configuration

Clients' computers could be either Linux based or windows based operating system. Clients are configured according to the server settings in order to benefit from its services. Each client is assigned a unique IP address provided by the DHCP server besides other parameters.

Each client was assigned a unique IP address provided by the DHCP server. As shown in Figure (8) and according to the DHCP server configuration the client got the following parameters, the connection DNS suffix is lab4.local, the IP address that was provided by the DHCP server is 10.66.77.4, the lease time that allocated to this client IP address, the DHCP server IP address and the DNS server which are the DNS server used by the mobile network as the Internet connection was established.

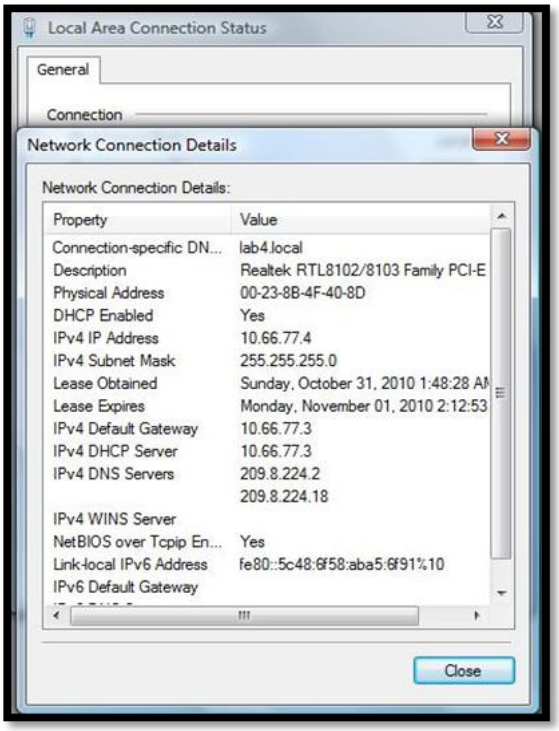

Fig. 8.DHCP Service Test.

The clients' browsers are modified according to the squid proxy setting. Squid proxy port besides its IP address are set by the clients, if the clients did not set these parameters, no Internet access would be available.

Clients should prove their authorization by entering a valid username/password as shown in Figure (9). Username is case insensitive spelling.

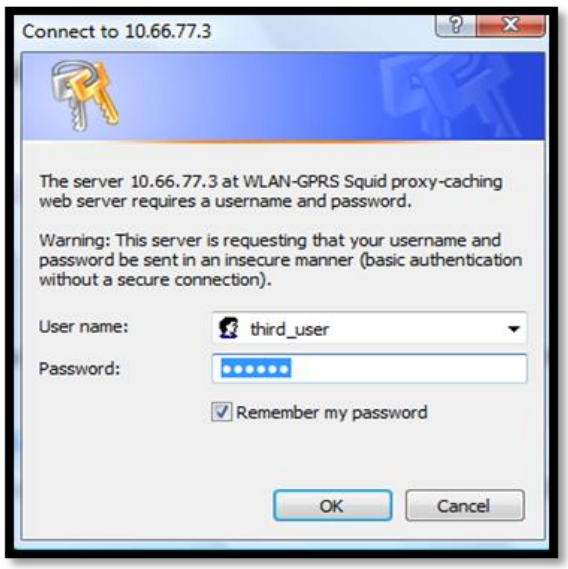

Fig. 9.Squid Authentication Announcement.

After authentication process, clients could access the Internet within the squid's rules. According to which time specification is allowed for Internet access, otherwise Internet access would be rejected by the proxy as shown in Figure (10). Besides time specification, access to Internet would be limited to particular web pages that may adversely affect the bandwidth and would be block downloading .wav or .avi file or www.hacker.com web page.

Fig. 10. Client's Request out of Allowable Time was Rejected.

Private Shell, Puttygen and Putty software are installed at clients' windows based computers in order to access the SSH server within the SSH tunnel. Only specified clients are allowed to access the SSH server those clients have to be configured with SSH server IP address and port. Features provided by the SSH server are:

a- Forwarding GUI programs: SSH can forward graphical applications over a network, extra software is required to forward programs to windows based operating system such as xming software. Xming is windows based X11 server/client software is downloaded and run at clients' host. As shown in figure (11) forwarding firefox application.

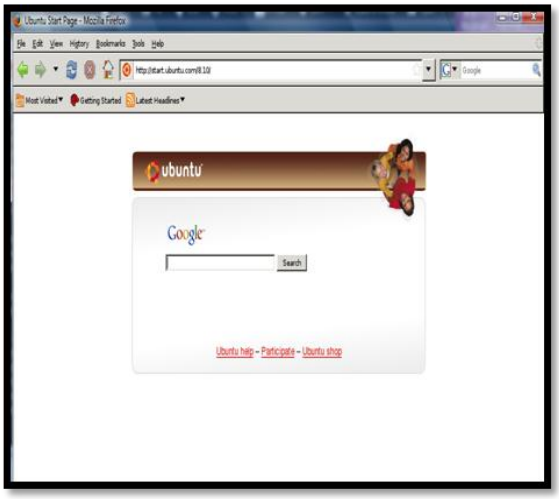

Fig. 11.Forwarding Firefox Application.

b- Dynamic port forwarding: Which would turn the SSH client into a SOCKS proxy server. SOCKS is a little known but widely implemented protocol by which any Internet connection request is done through a SOCKS proxy server, which encrypts the requested data.

In order to ensure that the traffic within the SSH tunnel is encrypted, the Wire shark software is used to sniff the packets. As shown in figure (12), a sample of captured packets through the SSH tunnel.

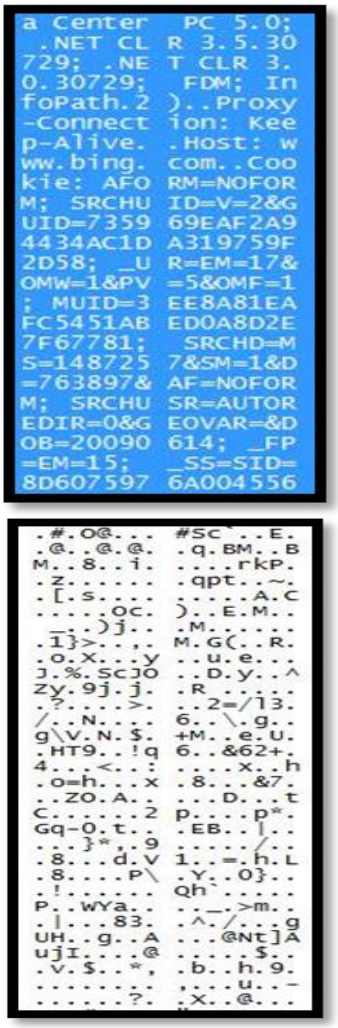

Fig. 12.Plain and Encrypted Packets within the SSH Tunnel.

4. Network Assessment

4.1. GPRS Data Transfer Rate

The data transfer rates are tested by uploading data to another network and downloading data from the same network. The GPRS getaway limits the uploading rate to approximately 40 Kbit/s and the downloading rate to approximately 60 Kbit/s.

The tests are done at the server computer which means that the tests are directly through GPRS connection. The data is transferred to www.testmy.net. The uploaded data size is 1013 KB and the downloaded data size is 1024 KB.

The data transfer rates are calculated using the equation:

((data size in bytes) * 8 / transfer time in seconds) / 1000 to get the transfer rate in Kbit/s

Four uploading and downloading tests are performed at different times of the day, The average uploading data transfer rate was 10.95 Kbit/s and the average downloading rate was 13.7 Kbit/s. Figure (13) depicted GPRS transfer rates for both upload and download.

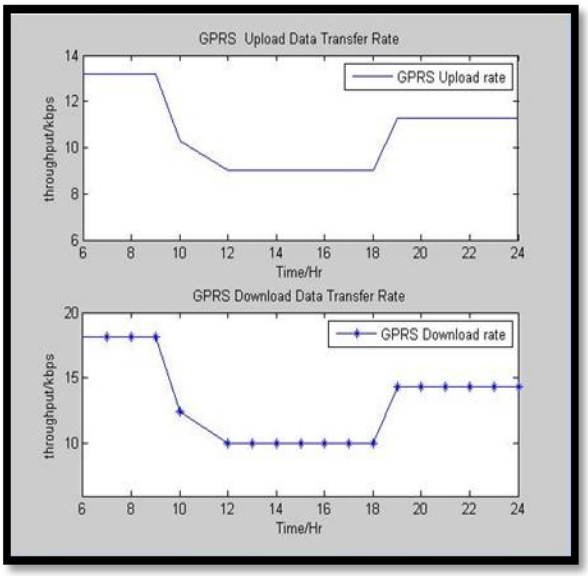

Fig. 13.GPRS Upload and Download Data Transfer Rates.

The results of uploading and downloading tests show that the GPRS bandwidth variation due to the signal fluctuations and the network traffic generated by other users especially at the network peak time within the period from 11:00 am – 4:00 pm. The average uploading and downloading data transfer rates are lower than the theoretical rates.

4.2. Network Performance Test

Performance test is done at the network in order to monitor how the GPRS connection at the server can handle the traffic generated by users and how Web browsing is affected. The test is performed by loading Web sites at the server and then requesting the sites at the client's host in order to test the operation of Squid Proxy cache and its performance enhancement. Fig.(14) shows the loading of www.ivsl.com site.

The site is loaded within 25 seconds with maximum downloading rate 6 Kbit/s and maximum uploading rate 5 Kbit/s. This site includes an image.

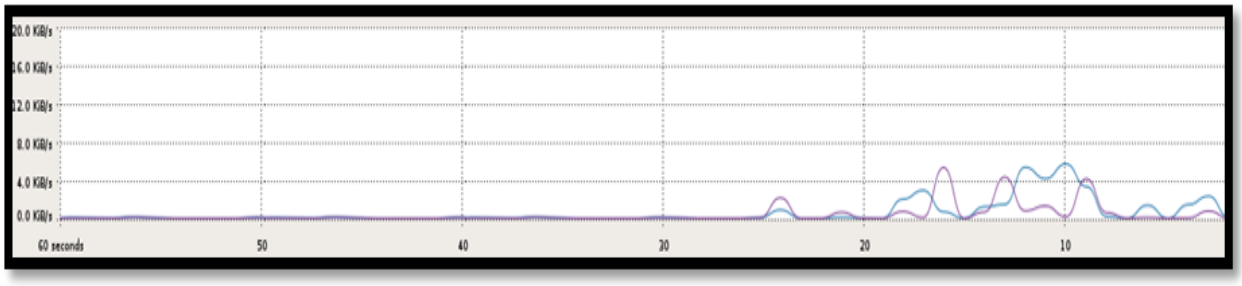

Fig. 14.Loading the Site at the Server's Host.

As the client requested that site, it was loaded within 4 seconds with maximum downloading rate 850 Kbit/s and maximum uploading rate of 150 Kbit/s. as shown in Figure (15).

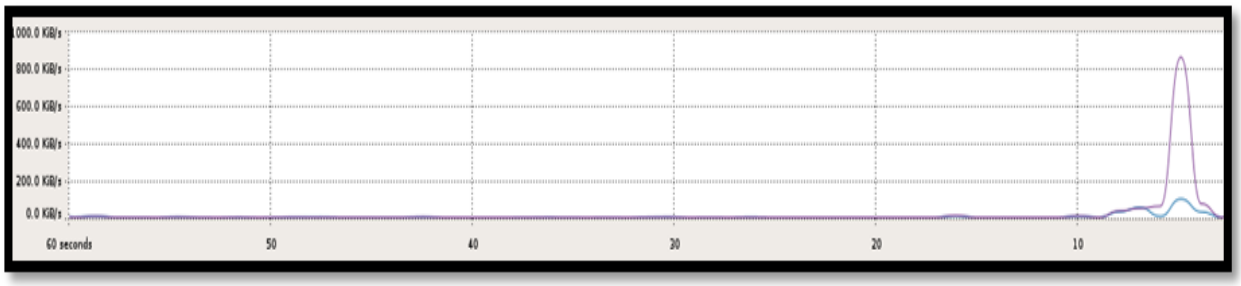

Fig. 15.Loading the Site at the Client's Host.

The network performance test reveals the importance of squid proxy existence. As the clients' requests could be loaded from the squid's cache if they were saved, this defiantly enhances the network performance.

5. Conclusions

Throughout the work a WLAN based on GPRS network to get access to the Internet was designed and implemented, the following remarks are concluded:

a- Accessing the Internet via a GPRS connection by the mobile station has many benefits such as smaller in size, easy to install, costless and mainly its wide coverage area especially for places that have no Internet provider available.
b- Due to the lack of available Public IP addresses that was required for the server and a specific clients in order to establish the SSH tunneling, Hamachi software was suggested to enable access to the server from remote clients.
c- In order to overcome the limitation of GPRS bandwidth provided by the mobile network operators, Squid proxy server was implemented to enhance the network performance. Besides its caching Squid Proxy Server restrict the users' activity while accessing the Internet by blocking some of the download features and specific sites.
d- Security considerations were paramount in the implemented network, that rely on three points:
e- Squid proxy server was configured to perform authentication process before allowing access to Internet, therefore any clients that does not belong to the network would not be able to attend the network and access the Internet.
f- By using SSH with Hamachi, a secure VPN was set up between remote clients and the Linux server.
g- By applying SSH with SOCKS proxy, the Internet traffic would go through a SOCKS proxy. This supports the security by having data encryption.

6. References

[1] M. Sauter, "Communication Systems for the Mobile Information Society", ISBN: 100-470-0267-6 (HB), John Wiley & Sons, Ltd, 2006.
[2] A. Mishra, "Advanced Cellular Network Planning and Optimization 2G Evolution to 4G", ISBN-13: 978-0-470-0147-4 (HB), John Wiley & Sons, Ltd, 2007.

[3] J. Eberspacher, H. Vogel, C. Bettstetter and C. Hartmann, "GSM Architecture, Protocols and Services", 3rd Edition, ISBN: 978-047-030707(HB), Wiley & Sons, Ltd, 2009.

[4] A. Jani, "General Packet Radio Service (GPRS)", IEEE potentials, Vol. 21, No. 2, pp. 12-15, 2002.

[5] T. Sohus and P. Nielsen, "Analysis and Model based Optimization of TCP for Wireless Networks", Master thesis, Distributed systems, Department of Control Engineering, Alborg university, Denmark, 2003.

[6] Zinah J. Ameen "WLAN Network based on GPRS Network" M.Sc. Thesis, Al-Nahrain University, College of Information Engineering 2011.

[7] LogMeIn, Inc. "LogMeIn Hamachi2 security white paper" 2011.

دمج شبكة لاسلكية محلية مع شبكة GPRS بشكل آمن

محمد احمد عبد الله* خليفة عبود سالم زينة جعفر محمد أمين*****

قسم هندسة المعلومات و الاتصالات/ كلية هندسة المعلومات/ جامعة النهرين

**قسم هندسة المعلومات والاتصالات/ كلية الهندسة الخوارزمي/ جامعة بغداد*

***قسم هندسة الحاسبات وتكنولوجيا المعلومات/ الجامعة التكنولوجية*

البريد الالكتروني:mohammedalmushdany@yahoo.com

البريد الالكتروني:khalifaabboud@yahoo.com

البريد الالكتروني:Zinahameen83@yahoo.com

الخلاصة

في هذا البحث تم بناء شبكة لاسلكية محلية لاستخدامها للدخول الى الانترنت من خلال شبكة GPRS الخليوية باستخدام منفذ دخول مربوط الى مقسم. تتم ادارة هذه الشبكة من خلال خادم تم برمجته باستخدام نظام التشغيل Linux. نظرا للامكانيات المحدودة التي توفرها شبكة GPRS مثل العنونة المتغيرة IP بالاضافة الى كون عرض الحزمة محدود لذلك تم اضافة عدد من التقنيات للتغلب على هذه المحددات. تم اضافة خادمDHCP ليكون المسيطر الوحيد الذي يتم من خلاله توزيع العناوين IP . ولغرض تقليل استخدام حزمة الانترنت تم اضافة خادم Proxy حيث يقوم بخزن الصفحات التي تم استدعاؤها في وقت سابق لغرض الاستخدام اللاحق و زيادة سرعة الحصول على البيانات من قبل المستخدم. كما ان اضافة مترجم العناوينNAT جعل بالامكان مشاركة نفس العنوان من قبل اكثر من مستخدم. نظرا لعدم سرية تبادل البيانات من خلال شبكة الانترنت لذلك تم اضافة بروتوكولSSH لتدعيم امنية النظام.

اظهر الاختبار الاول بان سرعة تنزيل و تحميل البيانات في اوقات مختلفة كان بمعدل 10.95Kbps للتحميل 13.7Kbpsللتنزيل خلال نقطة ألأتصال GPRS. كما اظهر الاختبار الثاني بان اداء الشبكة قد تحسن باضافة خادمProxy حيث وجد بان معدل سرعة البيانات 143.3 Kbps للارسال و 376.6 Kbps للاستلام.