EVALUATION OF GPRS ENABLED SECURE REMOTE PATIENT MONITORING SYSTEM

K Malhotra, S Gardner, D Rees
School of Electronics
University of Glamorgan
Pontypridd, CF37 1DL, Wales, UK
E-mail: kmalhotr,sgardner,drees@glam.ac.uk

KEYWORDS
Wireless Telemedicine, Secure wireless networks, e-health, Remote monitoring applications

ABSTRACT

This paper presents a methodology for monitoring patients remotely without geographical barriers using a General Packet Radio Service (GPRS) enabled embedded system. The motivation for this work is the realisation that remote patient monitoring and control is becoming a necessity and that mobile facilities need to be developed to meet the current and the future requirements.

The system architecture is described and performance has been evaluated in the context of data security needs. The suitability of the GPRS connectivity is considered in the context of the overall architecture and TCP/IP over GPRS has been shown to provide both a feasible and practical strategy. The results achieved compares the performance using both an insecure channel and one protected through the implementation of Secure Shell (SSH).

The embedded system has been developed using the Linux Operating System, as this allows the overall system footprint to be configured to meet the initial requirements. The future developments on medium to long term trend analysis are presented to show how the system can be developed into a useful "telemedicine" facility. This will revolutionise the overall quality of life of million of patients worldwide by creating a virtual consulting room.

INTRODUCTION

Increased requirements for health monitoring and the lack of available medical expertise in many areas of the world often require patients to travel to medical centres at considerable inconvenience and expense. Remote telemedicine has now become a real possibility, but the issues of data integrity and security over normal Internet channels causes concern. Furthermore, the use of mobile technologies for the implementation of such systems holds a great promise but these do bring their own security challenges [2] [12]. Previous studies have highlighted the need for telemedicine to be cost effective, secure and convenient [5]. However, the mobility restrictions imposed by the use of traditional landline carriers have been shown to be significant barriers to the practical adoption of remote services.
The development of embedded mobile technologies in the health care marketplace can be considered as both evolutionary and revolutionary. Successful monitoring of remote patients has been undertaken, but the possibility of controlling the overall patient environment is a major step forward.

The proposed architecture takes two main forms. One would be direct monitoring and control from a central server, the other the implementation of monitoring and control strategies at the local level, with supervisory control implemented from the central service point. The devised architecture is highly scalable, allowing implementation on systems across different platforms. It ensures near real-time response to critical conditions whilst allowing long term trend analysis concurrently.

In this paper, we present an analysis of near real GPRS traffic using both standard and secure methods and the affects of data transfer over the proposed methodology have been evaluated.

GPRS OVERVIEW

The General Packet Radio Service (GPRS) has a substantial geographical footprint in many countries. This coupled with the proliferation of international roaming agreements indicates the potential for this to provide the solution to the geographical barriers. TCP/IP over GPRS offers all the advantages of packet data networks, integrated with the internet and with data being charged on a "packet" basis, rather than on a time basis [1] [11].

The challenge in using GPRS as a channel lies in its very nature. It is designed for "bursty" traffic rather than continuous streaming of data and has a variable channel capacity. The network theoretically has a bandwidth of up to 171.2 kbps. However, this is reduced in practice due to a large number of known and unknown factors. The service providers do not tend to give all the 8 channels to GPRS data transfer and thus it is usual for it to be between one and four. Additionally, to ensure reasonable quality of service, the coding scheme implemented tends to be CS2 and the uplink and downlink channels are also dynamically allocated.

Proceedings 12th International Conference ASMTA 2005
Khalid Al-Begain, Gunter Bolch, Miklos Telek © ECMS, 2005
ISBN 1-84233-112-4 (Set) / ISBN 1-84233-113-2 (CD)

The impact of some of these factors can be seen below, with the different channel coding schemes being considered. In the radio interface there are four coding schemes: CS-1, CS-2, CS-3, and CS-4, providing decreasing error protection. Table 1 below shows the different data rates expected from all the four coding schemes.

Table 1: GPRS Coding Schemes

Scheme	Code rate (convolution coding)	Service data rate (kbps)	Maximum data speed (8 time-slots)
CS-1	1/2	9.05	72.4 kbps
CS-2	2/3	13.4	107.2 kbps
CS-3	3/4	15.6	124.8 kbps
CS-4	1	21.4	171.2 kbps

In addition, there are issues of modem class, which defines the number of channels that can be aggregated, depending on availability.

Some of these factors are under the control (through choice) of the user, but many are not. Probably the most difficult parameter to define is the number of potential concurrent users. This depends on several factors that are totally outside the control, or even knowledge, of the user. Thus we can say that the actual transfer rate for a GPRS connection depends mainly on three things which are as follows: i) the system: differences in transfer rate in one time-slot between operators, ii) the modem: the maximum number of time-slots supported by the modem and iii) traffic: depending on the load on the GSM system in the area where we want to use GPRS, the transfer rate can be less than the modem actually can handle because the voice calls have higher priority than GPRS connections in the GSM system.

One could consider other mobile channels, such as that provided by Mobitex [13] but the issues here include lack of roaming and difficulty in implementing TCP/IP over the channel. GPRS has several important features from an end user perspective which can be summarised as follows:-

Bandwidth & Cost Factor

With GPRS, the information is split into separate but related "packets" before being transmitted and reassembled at the receiving end. Packet switching means that GPRS radio resources are used only when users are actually sending or receiving data and thus network resources and bandwidth are only used when data is actually transmitted though it is theoretically said to be always connected [14]. This efficient use of scarce radio resources means that large numbers of GPRS users can potentially share the same bandwidth and be served from a single cell. Also, another advantage is the fact that the user is charged only for the amount of data transferred and not for the time he is connected to the network.

Connectivity

In theory, GPRS facilitates instant connections, providing immediate information transmission and reception. As no dial-up modem connection is required, GPRS users are often referred to be as being "always connected" [11]. This is not true in practice, as often users can be "knocked off" a channel if it is not used for a period or can be sent "keep alives" from the service provider, at a cost.

Secured Applications

The security function provides three main benefits: it guards against unauthorised GPRS service usage (authentication and service request validation); it provides user identity confidentiality (temporary identification and ciphering); and it provides user data confidentiality (ciphering).

NEW FACE OF TELEMEDICINE

Telemedicine is a way by which patients can be examined, investigated, monitored and treated, with the patient and the doctor located poles apart. Telemedicine has seen a tremendous growth in the recent years in countries like UK, U.S.A, Greece, Japan, Canada, Germany and now in developing countries like India where around 650 million people live in rural areas. The European Commission has defined telemedicine as “rapid access to shared and remote medical expertise by means of telecommunications and information technologies, no matter where the patient or relevant information is located”.

The new face of telemedicine is also needed due to an increase in aging population. The number of persons aged 60 years or older is projected to be almost two billion by 2050 [2]. As a result, patients don’t need to visit a hospital or their doctor so frequently which means lower health-care costs. It has been widely noticed that mobile devices are emerging as the ‘stethoscopes’ of next generation healthcare industry. An introduction of embedded internet technology in healthcare industry introduces cost-efficient systems with optimal performance, high confidence, reduced time to market and faster deployment. The internet is a medium to be considered because of ubiquity of the internet world. The device used for monitoring patients always needs to be connected remotely so GPRS has been considered for its “always on” capability. Thus, security is one of the major concerns as “always on” can mean “always vulnerable”.

Need of Security In Health Industry

Information security is a vital issue in the case of medical applications when the patient data is used for either real-time diagnostic purposes or long term analysis of chronic conditions.

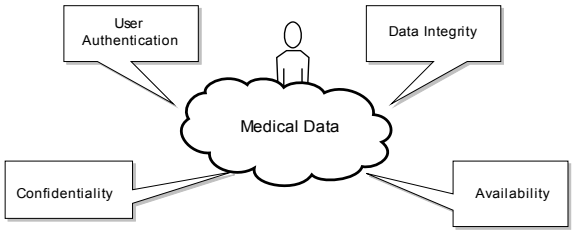

Figure 1: Components of security model

Figure 1 above showing the goals of securing a patient's medical data are as follows:

1. User Authentication: To provide privacy to patient data, the medical professional is validated using passwords, tokens, digital certificates or biometrics.
2. Data Integrity: To avoid data loss, corruption or malicious tampering issues, integrity of data is ensured by digital signatures and encryption algorithms.
3. Confidentiality: This does not only apply to transmitted data but also to "secrets" held by the devices and is achieved by cryptographic means. Upon the release of such information, there is the potential danger of harming a remote patient either physically or emotionally.
4. Availability: This ensures that the system can perform its intended function without being disrupted by various technical or malicious causes, such as mobile data service latency or Quality of Service problems.

Considering the sensitivity of patient data we have implemented a Secure Shell connection and the results obtained have been shown later in this paper. SSH has been freely available [6]. It provides an encrypted terminal session with strong authentication of both the server and client, using public-key cryptography facilitating file transfers and interactive downloading and uploading of files between patient side system and remote servers [9]. The SSH protocol provides authentication, confidentiality and data integrity thus fulfilling the main objectives of secure network as mentioned above.

Performance Issues

Performance issues are increasingly experienced by wireless network operators due to the limited capacity of networks [8]. Performance of a network is more important when a time critical application of telemedicine is taken into account. In case of telemedicine applications, the data sent across the network differ in its sensitivity to delays on one side and transmission error on the other. For patient data, delay should be avoided at all cost in order to preserve the continuity and order of the signals in the transmission. This is crucial for the data sent across the patient side to be acceptable by the remote doctor.

European Telecommunications Standard Institute (ETSI) [9] has specified four Quality of Service (QoS) classes for GPRS subscribers: (i) Delay which defines values for end-to-end packet transfer between two entities; (ii) Reliability which represents maximum values accepted by an application in terms of loss; (iii) Service Precedence which indicates three levels of priority for a service i.e. high, normal, and low. In case of congestion, a service with higher priority will receive a better treatment; (iv) Throughput which signifies the peak throughput in octets per second and the mean throughput in octets per hour at which packets are expected to be transferred across the network [2].

Transmission Control protocol (TCP) and User Datagram Protocol (UDP) are two Internet Protocol transport protocols that are used for transmitting data over the Internet as shown in Fig 2. TCP, a reliable protocol, guarantees delivery of all packets and in order which is quite useful in error-sensitive applications. UDP is designed for the quickest possible forwarding of data, without guaranteeing delivery of packets or the ordering of received packets useful for delay-sensitive applications. We have focused on TCP for reliability issues, an essential requirement for transferring patient data over wireless medium.

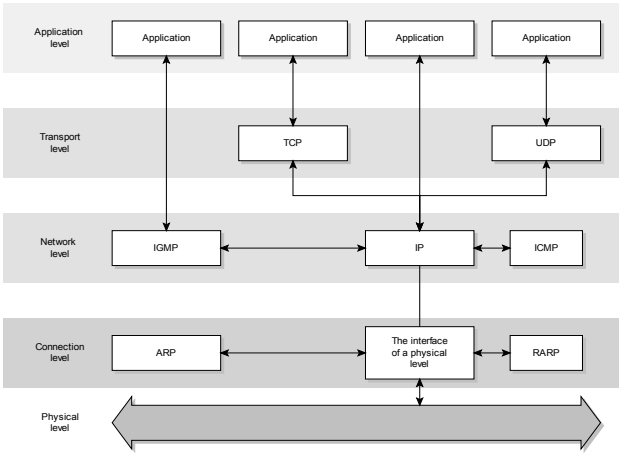

Figure 2: Network model based on TCP/IP protocols

SYSTEM ARCHITECTURE

The development platform has been created with both security and functionality as an integrated part of the initial specification. The remote communications are to be accessed by an authorised user (doctor), via a web browser, anywhere in the world. The communications for this are to be TCP/IP over GPRS, which facilitates IP communications at an acceptable data rate regardless of any mobility constraints.

The strategy to be implemented has been drawn from the functional and practical data transfer analysis and it has been decided that it is impractical to try to monitor and control the patient environment directly from a central point, if mobility is an issue. The channel has variability throughout the day; changes on different days and has a statistical variability that would make direct control an unstable proposition.

It has therefore been decided to implement a strategy which incorporates the required control functionality at the local level, whilst maintaining high level trend analysis using statistical process control (SPC). To permit total patient mobility, an embedded device has been integrated with the GPRS technology and an online data analysis system to create diagnosis features and an early warning system for life-threatening conditions. We have used the Siemens MC35 wireless module (4+1) having 4 downlink and 1 uplink channels, which delivers fast and reliable data and voice transmission over mobile networks.

In order for such systems to be accepted for general use, numerous technical and regulatory hurdles have to be overcome, and security is going to be one of the major issues. Security in this context is much more than just encryption. The security considered is at the system level. The GPRS link is only made on an event (practitioner use or data download), which makes it difficult to attack. The data is sent regularly to a central server and both server and controller can only be accessed via an authentication mechanism.

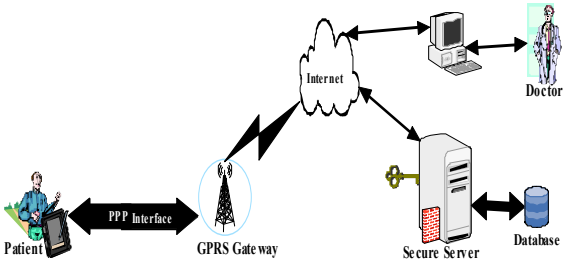

Figure 3: Secure Telemedicine System Architecture

The immediacy and directness of communication to the patient is supported by long term data storage, for audit and analysis purposes, on a secure central database as shown in Figure 3. The database updates can be set to occur on time or event interrupts. In addition, all recorded information can be transferred to secure servers via the Internet and seamlessly integrate into personal electronic medical record and research databases for archiving purposes.

The utilities running on the server can be used to monitor and to detect any changes in the patient's health over longer timescales and can alarm the appropriate professional to a degrading situation of the patient. This means that attention to a patient can be based on need rather than a scheduled visit, which is often difficult in remote locations.

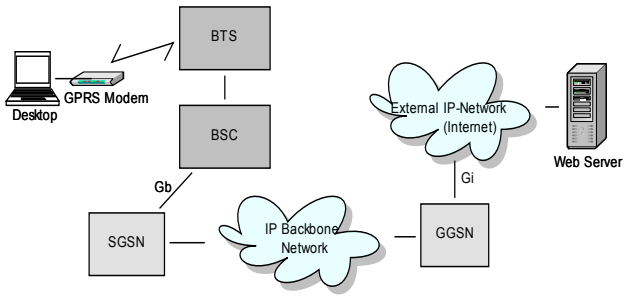

Figure 4: GPRS Network Flow

In Figure 4, GPRS internal network architecture is shown [1]. The GGSN (Gateway GPRS Support Node) acts as a gateway node to the internet world. An SGSN (Serving GPRS Node) is responsible for the delivery of packets to and from mobile station within its service area [2] [8]. It tasks include ciphering and authentication, sessions and mobility management.

High quality of service is also a major requirement for telemedicine and evaluations of the architecture have been implemented using both standard, cost-effective embedded Linux boards and very low cost microprocessors. The choice will depend on the application and will focus on things like the need for an Operating System for high quality local display and highly secure data encryption implementations.

DATA TRAFFIC ANALYSIS

The types of information to be sent will be application dependent. For example images may be required to be analysed and so compression techniques will need to be employed which allow high quality reconstruction at the practitioner. These will be high data volume applications, but the control and monitoring application will use significantly less data, in the order of a few Kb per transaction. We have focused initially on the text files and plain JPEG files without deploying any compression techniques.

The initial test configuration was implemented to measure the effects of varying transmission rates to and from a remote client. This corresponds to transmission from a remote patient to secure database and transmission from the secure database to the remote patient. The average transmission rates achieved over the test-bed were measured by transmitting a JPEG image and a known text file in near real-time environment.

The results are gathered while transmitting the data packets in real mode. The test rig has been used to

analyse the performance over GPRS transmission. The GPRS connection was made using Movistar SIM (a Spanish company providing GPRS infrastructure) which was placed in a GPRS modem. The connection was established over Point-to-point Protocol (PPP). PPP allows a remote access server to automatically assign an IP address, a default IP gateway to a dial-up client (a patient monitoring device). It provides error detection on the link itself. Its important feature is to allow negotiations between communicating sides, such as IP address and the maximum datagram size at start-up time, and also provides client authorization [4]. The moment the PPP authentication using Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) has been approved by the ISP located in Spain, a dynamic IP gets generated and the system gets connected to the internet. The data transfer rate of the Internet connection was then tested and the data packets were generated and sent across different systems. Due to the page limit of this paper, the scripts written and modified in the embedded system to make a secure connection will not be included.

Round Trip Time (RTT) using ping will get latency and the results gathered over diverse IP addresses pinged during different time of the day is shown in Figure 5 below. It gives a measure of the time it takes for a packet to travel from a system, across a network to another remote computer, and back.

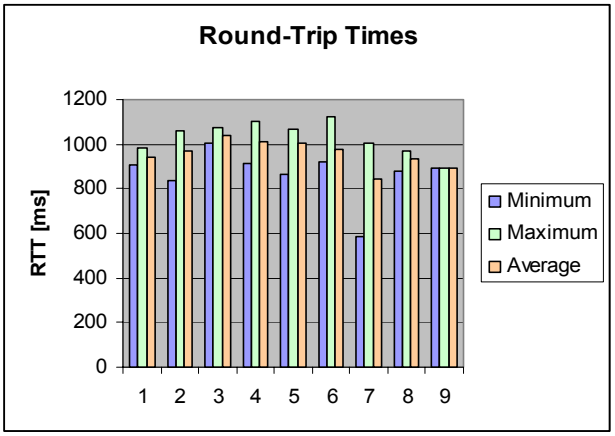

Figure 5: Round-trip time under real GPRS network

The result above shows the 'bursty' characteristics of GPRS traffic over different durations. The data rate achieved over GPRS medium during different duration of the day and during different events varies but it is sufficient for the successful transmission of the gathered patient's readings and for supervisory control.

The data transfer rates were tested by uploading the data files (text file and JPEG file) from the client machine which is considered to be patient monitoring system in our case, to the remote database server. The results were also obtained for downloading the same data from the server end. Ethereal [3] was installed on both the systems for statistical evaluation, which is a freeware network packet analyzer. The data was transferred using the file transfer protocol over GPRS connection. The size of the files that were used was approximately 100Kbytes. We have considered two types of files (text and JPEG) to show the variation of transfer caused due to different set of data.

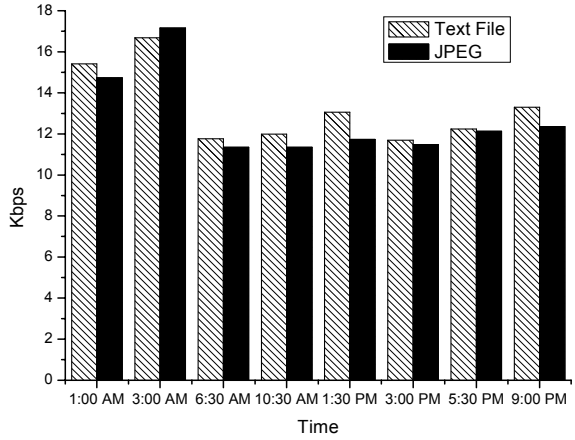

Figure 6: Variation of Upload Data Transfer Rate

In Figure 6, the uplink results of files transfer performed during different times of the day are shown. Thus, we can see that an average uploading data rate achieved during different time is 13.267 kbps for a text file and 12.787 kbps for an image file which will be acceptable for sending patient's data remotely during initial phases. The figure 7 shows the downlink results of the data packets transferred over remote systems. The average downloading data rate achieved during the experiment was 25.299 kbps for a text file and 24.537 kbps for an image file.

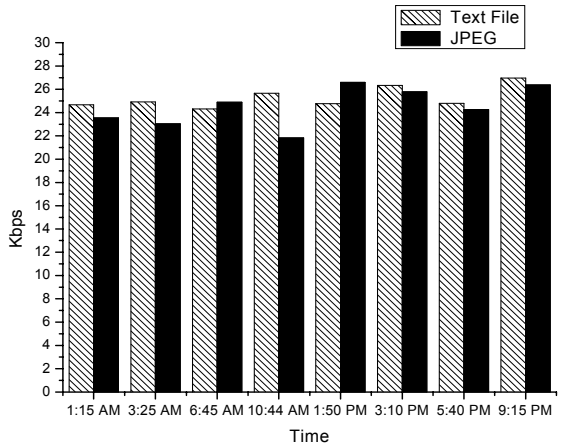

Figure 7: Variation of downloading Data Transfer Rate

The above result shows that the GPRS bandwidth may have significant variations over different durations of time. This is mainly due to signal strength fluctuations and the traffic generated by the other users.

In Figure 8, a time sequence graph is used to illustrate the general activity and events during the lifetime of the connection where we can observe the TCP traces; 'A' depicts the maximum number of sequences, and 'B' shows the upper and lower limits representing the sequence number of first and last byte in the segment. In an ideal condition the graph would be a straight rising line with its slope equalling the throughput.

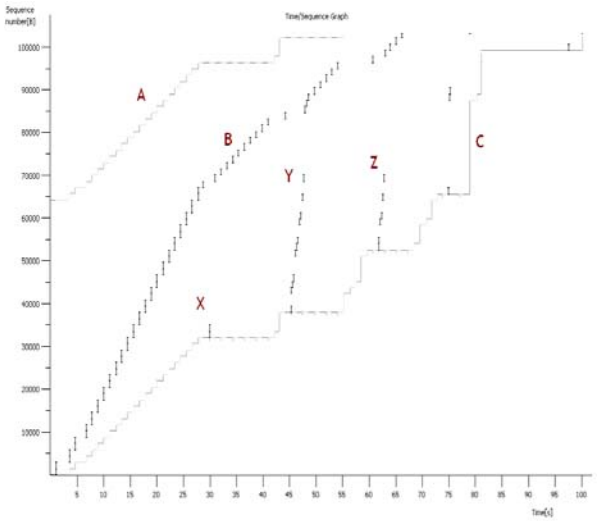

Figure 8: TCP Stream analysis using Time Sequence graph

The traces X, Y and Z show the data packets which require retransmission and thus affecting the throughput during this duration. The trace 'C' shows the acknowledgement returned by the receiver end. It has been observed that no segments are actually lost during the transmission process. It has been observed that TCP connection could not recover from the delay for its lifetime, unnecessary retransmitting many segments and thus acknowledging the successful transmissions.

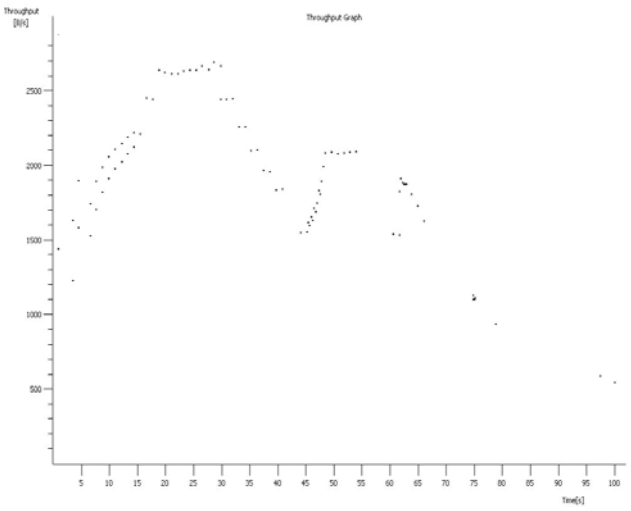

Figure 9: Throughput performance over time

In Figure 9, the overall throughput of the network is illustrated. Throughput in the figure varies and drop-off with time due to the retransmit sequence of packets. It has been observed that during the retransmission of packets in time sequence graph shown in Figure 8 there is a considerable fall in the throughput.

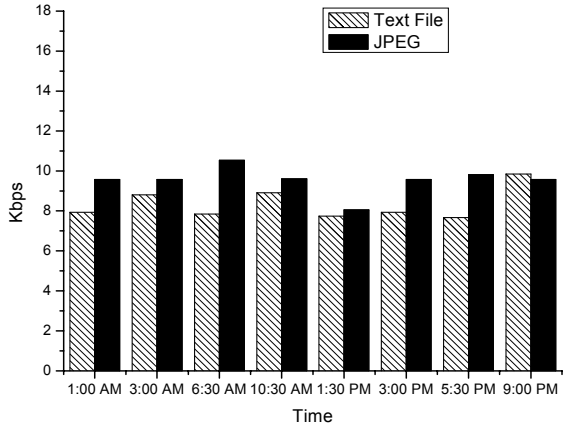

Figure 10: Uplink over secured medium using SSH

The figure 10 above shows the variation of data rate while uploading the files over secured shell. Secure shell uses 'sftp' (secure file transfer protocol) to transfer and receive the data packets. The average uploading data rate achieved over secured medium was 8.335 kbps for a text file and 9.541 kbps for an image file. We have observed that the data rate has been reduced as compared to the results shown in Figure 6 due to the introduction of encryption algorithms. The results in Figure 11 below show very little influence on the data rate of the implied security measures. The average downloading data rate achieved during the experiment in secured medium was 24.921 kbps for a text file and 25.762 kbps for an image file.

It has also been noted that the data rate for an image transfer in secured medium has improved over text file. This is due to the fact that the text file data is scrambled during transfer over SSH to improve data integrity.

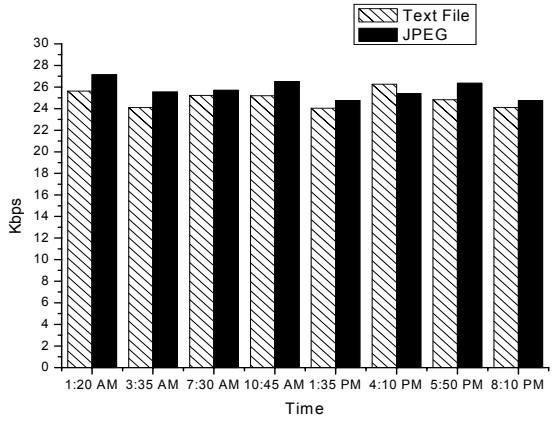

Figure 11: Downlink over secured medium using SSH

Thus, it has been observed that the use of GPRS technology for remote patient monitoring over secured medium can be reasonably deployed considering achievable data rates.

CONCLUSION & FUTURE WORK

We have observed that TCP did few retransmissions which cause the decrease in throughput. It has been observed that SSH deployment introduces small overhead in case of uploading data bundles but in the case of downlink it has been drastically reduced. We observed that this amount of reduction in the data transfer is acceptable as the patient monitoring application demands high level of security.

The results achieved also showed that the bandwidth of GPRS is limited due to various known and unknown reasons and we have to find out ways to maximize the performance of the connection through GPRS gateway. One of the good points which have been observed during the experiments is that GPRS connection once made never got disconnected unless done willingly. This will be useful while analyzing the remote patient data during different time intervals in a day.

The obvious advantage of using the above system is to avoid patient intervention while transmitting data to the remote server, which may result in irregular updating. However, no discussion of security will ever be complete and the only task is to deploy security and constantly evaluate known and emerging threats. The research carried out thus far has concentrated on developing a working system that allows the transmission of patient's data over secure wireless networks. This is a step toward producing a more flexible system that may transmit real time multimedia data over secure medium. The architecture discussed in this paper is the initial phase of the development of new era of telemedicine over wireless technologies. This work is part of our on-going research into the use of embedded systems in the healthcare sector. In this larger context, it is our first step in considering the security issues which plays vital role. To make this technology ubiquitous and accessible, a number of challenging issues needs to be resolved. These include overall system design, database rights, standardisation, security, privacy and legal concerns regarding professional accountability, particularly in relation to cross-border practice.

It has been noticed during the research that elliptic-curve cryptography (ECC) is been in demand for authentication, digital certificates, and public key encryption of the wireless devices, its implementation will be carried out in the future work.

REFERENCES

[1] P. Stuckmann, N. Ehlers, B. Wouters, *GPRS Traffic Performance Measurement*, IEEE Vehicular Technology Conference (VTC 2002 fall), Vancouver, Canada, 09/2002.

[2] B. Furht, M. Ilyas, *Wireless Internet Handbook Technologies, Standards, and Applications*, CRC Press, 2003.

[3] http://www.ethereal.com

[4] Olaf Kirch and Terry Dawson, *LINUX Network Administrators Guide,* O'Reilly, 2000.

[5] Woodward, B., Rasid, M. F. A., *Wireless Telemedicine: The Next Step?*, Proc. of the 4th Annual IEEE Conference on Information Technology Applications in Biomedicine, 2003.

[6] http://www.openssh.org

[7] Xiaohua Chen and David J. Goodman, *Theoretical Analysis of GPRS Throughput and Delay*, IEEE International Conference on Communications, June 2004.

[8] T. Halonen, J. Romero, J Melero, *GSM, GPRS and EDGE Performance, Second Edition*, Wiley, 2003.

[9] *Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS) Service description; Stage 2*, 3GPP TS 03.60 version 7.7.0, Release 1998.

[10] Daniel J. Barrett and Richard E. Silverman, *SSH, the Secure Shell: The Definitive Guide*, O'Reilly, 2001.

[11] C. Andersson, GPRS and 3G Wireless Applications, Wiley, 2001.

[12] I. E. G. Richardson, M. J. Riley. W Haston, I Armstrong, *Telemedicine and teleconferencing: the SAVIOUR project*, Computing & Control Engineering Journal, Feb 1996.

[13] http://www.mobitex.org/

[14] S Buckingham, *What is General Packet Radio Service?*, January 2000 accessed on November 2004 from http://www.gsmworld.com/technology/gprs/intro.shtml