Algorithms Research 2012, 1(2): 5-11
DOI: 10.5923/j.algorithms.20120102.01

Algorithm Re-Ordering: a Solution for Abating Internet Bypass

Awoleye O. M*, Atoyebi M. K, Abang I. S, Siyanbola W. O

National Centre for Technology Management, an Agency of the Federal Ministry of Science & Technology, Obafemi Awolowo University, Ile-Ife, Nigeria

Abstract The use of mobile data services as a means of communication came into existence through the introduction of 3rd Generation (3G) Technology, it is expected that this technology will continue to increase opportunities for improved revenues and enable new services & tariff generation. Research have shown that the use of third party application like Tor browser, Indian proxy, Your-freedom (http://www.your-freedom.net), Privoxy etc are used to bypass the data services offered by the network providers. This is carried out by leveraging on virtual private network (VPN) technology, distributed network of relays and available free ports. This has limited the revenue derived by the providers in a country where such proliferation is thriving. In Nigeria for example Government on its part have taken some steps to finding solutions to end this menace and related increasing cyber crime activities, but the challenge still remain with us. This work thus postulates an innovative way of abating this activity which has lead to huge loss of revenue in the sector. The approach is a theoretical method in solving the industry-related problem. It narrowed down the problem of the current algorithm to improper algorithm order and thereby proposing an appropriate model to reducing the menace.

Keywords Algorithm, flowchart, policy, internet, data services

1. Introduction

History reveals that the mobile/wireless telecommunication could be traced back to the laboratory research carried out in United State in the 1920's by means of radio telephony technology[1]. This has been suggested to be the most important device of the mobile telecommunication and as the key element to enable mobile and wireless access[5,7].

The initial design of the mobile telephone was based on analogue which was characterised as the first generation (1G) of mobile phones. It was designed to carry voice only, which was then the primary function[17]. The mobile telephone has gone through a number of developmental cycles up to the advent of migration from 2G to 3G technology that have increased the market base of the network operators worldwide. There have been considerable increases in the investment on infrastructure expansion in the telecommunication industry over the years due to continuous growth and increased market demand[3.5]. Technological innovations in the transmission and switching technologies have also been reported to aid cost reduction, as well as improve accessibility of existing telecommunication services[1].

In addition, deregulation of the telecommunication industry has made the market more competitive, this combined with technological advances that have resulted in a diversity of new services, most especially data transmission and video applications[2,3]. The extensive use of these services and its adoption, especially the wireless data service cannot be overemphasised. This has presented an avenue for the providers to tap into new opportunities of revenue generation in the industry. Surprisingly, despite the huge benefits of providing these services coupled with the exorbitant amount of such investments from the provider's side, saboteurs are beginning to ravage some of the revenue that could accrue to the providers. Beyond gainsay, it has been established by the evidences around that some prepaid data service subscribers still have access to the internet even when their credit is below the threshold set by the providers to gain access to the service. This thus set us thinking about the future of this industry and some research questions are raised which this work will attempt to answer. It is expedient to raise an issue of sustainability in an arena of looming uncertainty. These questions are: (i) Will the wireless data service providers be willing to continue in the near future when the investment/overhead is no longer commensurate to revenue? (ii) Will the futility of the struggle of the providers to abate Internet by-pass kick them out of business without a reasonable solution? (iii) Is there any alternative solution (technical and non-technical) to abate this menace? This has been carefully attended to by employing algorithm and using policy suggestions as a veritable instrument of control to safe the situation. This is a theoretical approach of solving an industry related problem in Nigeria.

* Corresponding author:
awoleye@yahoo.co.uk (Awoleye O.M)
Published online at http://journal.sapub.org/algorithms

It is worth noting to state that a number of third party software are used in carrying out this nefarious activities. Example of which are: freedom server, tor browser, ultra surf to mention a few, have been used extensively among the perpetrators. Freedom server for example has specifically listed the service providers in Nigeria with their corresponding by-pass proxy configurations and port numbers to enable data services on the third party provided network. Riding on the platform provided by the local service provider in Nigeria to access another remote system for service provisioning contrary to terms of use is viewed as a major algorithm order loophole. This is blamed on the local service providers who could not secure their network appropriately. Security has proved to be an essential aspect of telecommunication as exemplified by the inclusion of authentication of mobile terminal by the network which stopped the massive fraud that was occurring in the previous generation of analogue mobile system[14]. Attempts have been made by some of the service providers to stop this menace but it seems to be of no avail. The approach adopted mostly is to change the Internet Protocol (IP) addresses of their web proxy and related servers. This study thus employed the use of algorithm to illustrate the steps that must be taken to mitigate data service by-pass. It therefore set three objectives to achieve a main goal of preventing by-pass of data services provisioning. These are to: (i) examine the current procedure for mobile call service on how the service providers carry out this primary function; (ii) review the data service procedure with a view to present an alternative; and (iii) to advance some useful policy directions to prevent future occurrence(s) in the industry.

2. Methodology

The approach adopted in this research is the use of flowchart to elicit the loop-holes of the telecoms operators' activities in Nigeria with a view to proffer a suitable measure to overcome the limitations. To achieve this, a framework (flowchart and pseudo-code) were designed following an extensive literature search on the procedure employed by network operators for their voice call and data services. The research thus redirected the procedure to censor the infiltration of proxy browser users. This is to create a secure mode for data communication and tackle the concern of revenue loss.

3. GSM to GSM Call Initiation

Mobile technology's original function was to perform voice service only[15]. Fig.1 depicts the process of making a GSM to GSM call. This starts from the Mobile Station (MS) initiating a call by sending a request on the Request Access Channel of the Base Station Subsystem (BSS). The BSS responds with Base Transceiver (BTS) to the MS using the Assignment Channel (present in the antenna). The process is carried out so as to allocate a specific voice channel to MS. The BSS then send a request to the Mobile Service Switching Centre (MSC), thus this initiates a call. The MSC perform the necessary authentication with the aid of the Home Locator Register/Visitor Locator Register, Authentication Centre and the Equipment Identity Register. The Home Locator Register (HLR) holds the Subscriber Identity Module (SIM) information and its associated location. The Authentication Centre (AUC) verifies the SIM to identity, the Equipment Identity Register perform the verification of the Mobile Equipment (mobile Phone). After the authentication, the MSC check the threshold value of the callers SIM to ensure the value is at least a minimum value to initiate the call. The MSC thereafter sends a message to the BSS of the called party. The BSS verifies the called party to ensure it is within the coverage area, otherwise it checks whether or not the called party has a voice mailbox activated. If it is not activated it terminates the call, but if voice mailbox is activated it prompts the caller to drop a message for the called party, but if the user is within the network coverage area, a signal is sent to the caller that his destination has been reached. In some instances the user might be on a call and the incoming call would be terminated unless he activates the call waiting service, which function is present on the network operator's end and also on the mobile equipment, the caller gets a call waiting request on the screen of his phone[8]. At the end of the conversation either of the party can terminate the call; in fig. 1 the called party end the call. The called mobile send a disconnect message to the BTS using the Fast Associated Control Channel. (FACCH), the FACCH is present in the antenna. The BSS then forward this message to the MSC, which then channel the request for termination to the callers BTS[5]. The BTS respond by sending release message down to the MS, the MS then respond by sending a message back to the BSS, which then send a release complete message to the MSC. The MSC then control the BSC to free that channel for any available user or release the BTS from the traffic channel (TCH) which is also present in the BTS[14,15].

3.1. The Procedure for Mobile Wireless Data Service

The advent of 3rd generation technology gives rise to Data service which comes either in circuit data or packet data[4]. This process is initiated when the user clicks on the connect button to request for a network connection through the modem which is connected to a computer. The modem then sends the user request to BSS through the BTS. The BTS directs the modem to dial the Internet service provider's (ISP's) phone number which is answered by another modem at the receiving end. The modem sends a control signal back and forth harmonizing connection between the user and the ISP's modem to determine the connection speed. Once the connection(speed) is established the mobile service switching centre (MSC) which consist of Authentication Centre (AUC) and the Home Location Register (HLR) send the username and the password to the ISP, using a process called

Challenge Handshake Authentication process (CHAP) as shown in fig 2[8]. The GPRS Support Node (GSN) checks the username and password against the database of the active subscriber and check the threshold value of the subscriber's bundle, once this condition is satisfied then the connection is established. After the connection has been successfully established, the browser then sends the HTTP client request to the server. The server upon receiving the request generates the requested file and begins the transmitting process[4].

```
START
Initiate a call;
IF BSS User <= 90 THEN
   Dialed digit connected to BSS;
   BSS sends the information to the MSC
ELSE
   Handover (transfer) to a free BSS;
   BSS sends the information to the MSC;
END IF
   MSC accepts the codes from BSS and send it to the EIR;
IF the Equipment IMEI is OK   THEN
   IMEI   Send  AUC;
        Info
ELSE
   Blacklist THEN
   Reject call: STOP
END IF
IF   SIM IMSI is OK   THEN
   Authenticate SIM
   AUC   send   HLR;
         info
ELSEIF
  Credits >=threshold value? THEN
  Pass control to BSS2
 ENDIF
ELSE
   SIM barred, damaged, not registered etc, STOP
END IF
IF the receiver is on HLR THEN
   Connect call to the receiver's BSS
ELSE
   Copy SIM information to VLR
   Connect to the receiver's BSS;
END IF
IF the Receiver is in coverage area THEN
   Connect call;
ELSE
IF Voice mail-box activated THEN
    Message sent to voice mail: STOP
ELSE
   Call terminated
END IF
ELSE
   Call terminated
END IF
IF call waiting is activated THEN
PRINT call waiting on MS
ELSE
   Terminate call
END IF
STOP
```

Figure 1. Initiating a GSM – GSM Call

```
START
    User request for connection through BTS;
    The BTS sends the modem request to the BSC;
    The BSC then forward the request to the EIR in the MSC;
IF The modem IMEI is OK   THEN
    BSS sends a request to the AUC
ELSE
    Modem blacklisted;
    Connection not established;
PRINT "err msg"
ENDIF
IF IMSI is OK THEN
  Credits/bundle >=threshold value? THEN
 Pass control to BSS
ELSEIF
  Is Traffic Channel available THEN
  MSC/GSN assigns channel to modem
  Network handshake established;
  Connection established (authentication successful);
ELSE
  BSS handover modem to a free BSS
END ELSEIF
  SIM barred, SIM not registered etc;
PRINT "err msg"
ENDIF
  Connection terminated;
STOP
```

Figure 2. Current Data Service

3.2. Description of a Typical Data Service by-pass

Owing to the various benefits associated with the use of new technologies, there has been increasing demand especially for data services which gives access to surfing the Internet. This had left the service providers with the various challenges of meeting their high rising demand. The focus of these service providers had been prioritized on their ability to meet up with the demand of their subscribers with little or no attention on the security aspect of their network. The procedure to connect to the data service, especially the pre-paid billing plan requires a dial-up via the computer. When the request to connect is made, the system checks all the necessary conditions for authentication, if all the conditions are fulfilled then authentication is granted. It is worth noting to state here that even when the condition for balance on credit request is not met, the system still allow the authentication to be granted though with a limitation to transmit data on the provider's server. This is where the loophole is, authenticating the modem without having enough credit balance has given the modem the opportunity to ride on this platform to a third-party server. The third party server will thereafter take it over from there and provide the data service to the subscriber. Although the data service provided is at no cost to the local service provider who originally provides the modem, but the overhead to sustain the modem online is borne by the local service provider. Some subscribers have noticed this loophole and have capitalized on it. Some have even commercialized this nefarious activity and are introducing other subscribers to it. If this should continue freely without any check, there is a likelihood that the service providers will be out of business. This is possible when all loyal subscribers are no more subscribing for their service. When the overhead being consumed on their proxy server is not paid for; this will eventually lead to huge revenue loss. This is actualized especially when the subscribers who are suppose to recharge

their access refuse to do so and yet are given access to login successfully, although with limitation to surfing the Internet. To reiterate this process, successful login is all that is needed to link up with other remote server which provides access through either a VPN or an external proxy access. For example, 'your-freedom.net' provides different price plans as shown in Fig 3.

	Free	Basic	Enhanced	Total
Bandwidth	64 kbit/s	256 kbit/s	4 Mbit/s	unlimited
Concurrent Streams	10	50	100	200
Web Proxy	✓	✓	✓	✓
SOCKS Proxy	✓	✓	✓	✓
OpenVPN mode	✓	✓	✓	✓
Link encryption	✓	✓	✓	✓
HTTP connection	✓	✓	✓	✓
HTTPS connection	✓	✓	✓	✓
CGI connection	✓	✓	✓	✓
FTP connection	✓	✓	✓	✓
UDP connection	✓	✓	✓	✓
Relaying permitted	✓	✓	✓	✓
Connection time	6 hours*	unlimited	unlimited	unlimited
Server Ports	✗	✗	✗	✓ (5)
1 month package	**FREE**	**€ 4.00** (NGN 846.87) (USD 5.11)	**€ 10.00** (NGN 2117.17) (USD 12.77)	**€ 19.99** (NGN 4232.23) (USD 25.52)
3 month package	**FREE**	**€ 10.00** (NGN 2117.17) (USD 12.77)	**€ 28.00** (NGN 5928.08) (USD 35.74)	**€ 57.99** (NGN 12277.48) (USD 74.03)
6 month package	**FREE**	**€ 17.00** (NGN 3599.19) (USD 21.70)	**€ 50.00** (NGN 10585.86) (USD 63.83)	**€ 109.99** (NGN 23286.77) (USD 140.41)
12 month package	**FREE**	**€ 30.00** (NGN 6351.52) (USD 38.30)	**€ 95.00** (NGN 20113.13) (USD 121.28)	**€ 199.99** (NGN 42341.32) (USD 255.31)

Source: *http://www.your-freedom.net/index.php?id=114*
Figure 3. price plans (packages) for remote data service

There is a provision for a free access with the limitation of 15hrs per week; a non-restrictive access is given at a fee depending on the price plan of choice. All of these plans are relatively cheaper than available in any developing countries. For example on the same figure, a bandwidth of 256kbit/s is allowed for the *basic* plan which cost less than a thousand naira (<N1,000) this is equivalent of about $5 with unlimited connection time, coupled with no limit on data that can be transferred. A 4Mbits/s is also available with the same facility for an *enhanced* package, this only cost about twice the price of the former. Whereas in Nigeria, a 200MB on average is priced at N1,000 (about $6) with a validity period of 30 days, but experience have shown that one can exhaust this in a day or two. With this, a regular user will need an average of at least N15,000 (over $90) monthly if the user is consuming an average of 100MB per day.

Let us consider an hypothetical example of all the service providers in Nigeria loosing just 1% of the total data service subscribers which is 6.2million as at the last count in 2011. A sum of N893million naira ($5.6million) would have been lost in a month. If this is calculated over a one year period, it will amount to N10.7trillion ($67million). This translates to a little more than 8 times the amount needed for fuel subsidy in Nigeria for the same period of one year.

3.3. Framework for re-ordering the Data Service

Fig. 4&5 presents the pseudocode and flowchart respectively for the new thinking to solving the problem of the by-pass in the data services provisioning. The process is initiated by connecting the modem to the computer, the Base Station Subsystem (BSS) which comprises the Base Station Controller (BSC) and the Base Station Transceiver (BTS) directs the modem to dial the Internet service provider's (ISP's) data service dedicated phone number which is answered by another modem at the receiving end. The modem then send a control signal back and forth harmonizing connection between the user and the internet ISP's modem to determine the connection speed. Once the connection (speed) is established the mobile service switching centre (MSC) which consist of Authentication Centre (AUC) and the Home Location Register (HLR) send the username and the password to the ISP using a process called Challenge Handshake Authentication process (CHAP) as shown in fig 4[6,9].

```
START
        User request for connection;
        The BTS sends the modem request to the BSC;
        The BSC sends a message to the EIR in the MSC;
        IF
            The modem IMEI is OK THEN
            BSS sends a request to the AUC
        ELSE
            Modem blacklisted;
             Connection not established;
             Print "err msg"
        ENDIF
        IF IMSI is OK THEN
        Local connection established
        Is Traffic Channel available?
        MSC/GNS assigns a channel to modem;
        Network handshake established;
            Connection established;
            ENDIF
            ELSE
            Handover modem to a free BSS (repeat the traffic test)
              ELSEIF
                Credit/Bundle >= threshold value THEN
                MSC/GNS assigns a channel to modem;
                Network handshake established;
                Connection established;
              ELSE
                  Cannot establish connection
              ELSE
                SIM barred, SIM not registered etc;
               Print "err msg"
               ENDIF
        ENDIF
            Connection terminated;
    STOP
```

Figure 4. Framework for Re-Ordering Data Service Connection

If the result of the authentication process is successful, the result is put onto stack and released when the following checks are satisfied. The system checks for IMEI, if it's okay, then the control will be passed on to check for the status of the IMSI as well otherwise SIM is reported bared or damaged. Successful check on SIM validation will prompt the MSC to check the balance on credit or the bundle if it's enough to get connected to the data service. Once this is satisfied and traffic channel is available then MSC assigns channel to modem and the connection is established. The

system must constantly continue to monitor/count down on the balance of the credit on SIM, once the credit is below the minimum set – the connection will be terminated.

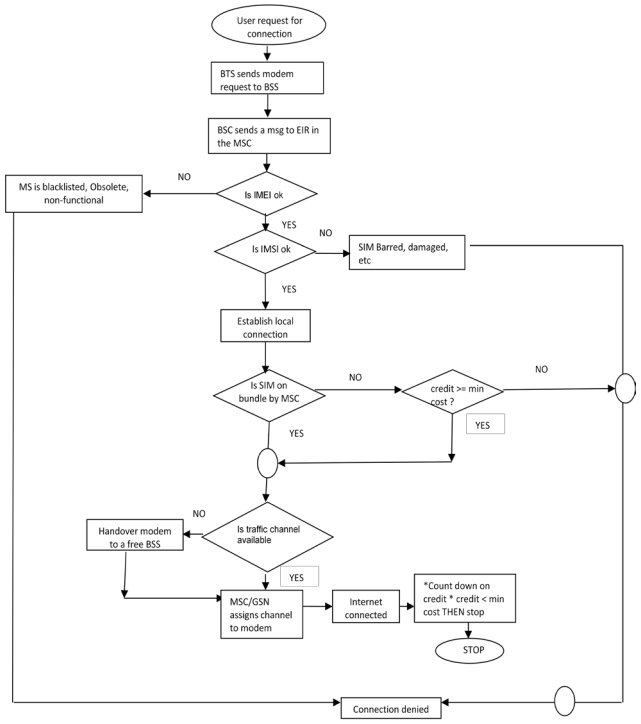

Figure 5. Framework for re-ordering data service connection

4. Conclusions

This study identified a major industry-related loophole in the telecoms industry in Nigeria. This has to do with a flaw in the algorithm order of the pre-paid wireless data service. This gives the opportunity to subscribers to use their network as platform to link to other data service provider, thereby making local service providers to lose revenue to their counterparts out of the shore of the country. The major concern in addition to revenue loss is the question of sustainability and continuity for the local service providers if this practice is not curtailed. This work also studied the existing GSM to GSM call service as well as the data service in order to identify the point of the algorithm error. We thus found that providing data service to the pre-paid subscribers, they are allowed to authenticate even when the remaining credit balance does not meet up to the required value to surf the Internet. Though the system restricts access to the same for data transfer as a second level access check. Investigation thus revealed that the first level access/authentication is all that is needed to connect to a third party service provider to link the subscriber to the Internet. The third party provider thus provided some parameters to the user's browser to redirect its request to a given proxy server and different port number. Others have also achieved this by providing software that will connect the user's machine in a virtual private network. This work therefore has presented a new procedure that will re-order the pre-paid billing & connect algorithm. The first level access to authenticate is not granted unless enough or the minimum credit balance is detected before access is granted. This presentation will follow what is at the moment operational with the prepaid call service. With the prepaid call service, once your credit is exhausted you are not allowed to connect. If this procedure is copied to the pre-paid wireless data service then the chance of overcoming the age long menace stands strong.

5. Policy Recommendations

It is expedient that this anomaly is corrected hence the providers will suffer for it and in return it will impact the countries' GDP. This is possible when the perpetrators network continue to grow and in return shrinks the number of loyal subscribers to the local service provider. To this end a number of policy recommendations are therefore advanced in this direction, and the ideal role for the key players, i.e the service providers, the government and the citizens (subscribers) are reiterated.

The service providers must include a clause to bind the subscribers and users of their products and services to exclusively use it for the purpose and their service alone. Any defiant should be forewarned and threatened with SIM barring and possibility of prosecution. If this already exists in the terms of use then it must be enforced, and reminder should be sent to subscribers at intervals. They can also make the subscribers to occasionally re-affirm their loyalty before access is granted. If this is done, there will be enough evidence tenable in court against any defiant. Once this is put in place then it becomes binding on the users and this will serve as deterrent especially when a few offenders have been punished. In addition, the service providers also should be given incentives to loyal subscribers such that if they have been loyal to their subscription for 11months then the 12^{th} months be given free. This way, subscribers will not exert their energy looking for ways to defraud them or looking for alternative ways of by-passing the payment. They should also at regular interval carry out analysis on the usage i.e. traffic flow on their network relative to income generated within a certain period. This promises to show some hidden pattern especially when data mining principles are employed. Some of which amongst others are possibility of outliers, which ordinary inspection cannot reveal. If any outlier is noticed then it must be thoroughly investigated. A public domain can also be created which will facilitate reporting of any act of indiscipline on a named network. Individual service providers can dedicate a sub-domain for this on their websites.

The government too on their part should play a supervisory role by ensuring that the service providers deliver their promises with good quality of service. They must also ensure that the citizens are not extorted with unreasonable cost on the services. Since liberalization of the sector which is over ten years now, it is believed that by now the cost of the services should be relatively affordable and cheap. Then the

government in return should further provide enabling environment for the smooth running of their services, such as provision of stable electricity which will go a long way in saving the cost of alternative power generation which the service providers are already incurring. The government also should also cut down on the tariff imposed on the service providers.

The subscribers also should be advised to act responsibly and should know that to keep those services available and running smoothly they have to play supportive role by paying correctly for the services.

ABBREVIATION

GSM: Global System for Mobile communication
BSS: Base Station system
BSC: Base Station Controller
BTS: Base Transceiver Station
GPRS: General Packet Radio System
3G: Third Generation
2G: Second Generation
PC: Personal Computer
MS: Mobile Station
SIM: Subscriber Identity Module
AUC: Authentication Centre
EIR: Equipment Identity Register
HLR: Home Location Register
VLR: Visitor Location Register
USRP: Universal Software Radio Peripheral
FACCH: Fast Associated Control Channel
TCH: Traffic Channel
ISP: Internet Service Provider
GSN: GPRS Support Node
HTTP: Hyper Text Transfer Protocol
CHAP: Challenge Handshake Authentication Process
IP: Internet Protocol
PPP: Point-Point Protocol
MSC: Mobile Service switching Centre
IMSI: International Mobile Subscriber Identity
IMEI: International Mobile Equipment Identity

REFERENCES

[1] Agar J. (2003). Constant Touch, a global history of the mobile phone Icon Books UK, Duxford, Cambridge, UK. Retrieved on 19th August 2011 from http://books.google.com/books/about/Constant_touch.html?id=mD7qPgftraMC

[2] Awoleye O.M., Siyanbola W.O., and Oladipupo F.O (2008). Adoption Assessment of Internet Usage amongst Undergraduates in Nigeria Universities- A Case Study Approach. *Journal of Technology Management and Innovation.* Vol 3(1), pp 84-89. Available onhttp://www.jotmi.org/index.php/GT/article/view/cas11/121

[3] Bateni M. H., Hajiaghayi M.T., Jafarpour S. & Pei D. Towards an Efficient Algorithmic Framework for Pricing Cellular Data Service. Retrieved on 25th January, 2012, available on http://www-math.mit.edu/~hajiagha/pricing.pdf

[4] Flippo O.E., Kolen A.W.J., Koster A.M.C., Van de Leensel R.L.M.J.(2000) A dynamic programming algorithm for the local access telecommunication network expansion problem. European Journal of Operational Research Vol.127, pp 189-202. Available on http://www.math2.rwth-aachen.de/~koster/paper/flkokole00.pdf

[5] Brahim G. & Luigi L.(2000). Understanding GPRS: The GSM Packet Radio Service published in: The International Journal of Computer and Telecommunications Networks - Special issue on future wireless networks archive Volume 34 (5). Retrieved on 18th August, 2011 from http://dl.acm.org/citation.cfm?id=364043

[6] Buckingham S. (1999). Data on GPRS, Mobile Life streams Limited. retrieved on 21st August, 2011 from http://lotos.site.uottawa.ca/ftp/pub/Lotos/Papers/GPRS_Tutorial.pdf

[7] David AB & Harvind SS (2008). The Open BTS Project: Signal Processing, Inc. Fairfield California, US. Retrieved on 19th August, 2011 fromhttp://www.cs.ru.nl/fabianbr/scriptie.pdf

[8] Dirk P (2002). GSM Radio Interface. Retrieved on 18th August, 2011 from http://www.aws.cit.ie/personnel/dpesch/notes/GSM_radio_interface.pdf

[9] Frank S, Chao-Chi H, Richard K, Arye E & John W (2010). Emergency Telecommunication Retrieved on 23rd August, 2011.

[10] IBM User Guide (2010). Security Network Active Bypass. Retrieved on 20th August, 2011 from http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/topic/com.ibm.ips.doc/pdfs/ProvNetworkActiveBypassUG.pdf

[11] Kellogg M., Thorne J. & Huber P. (1992). Federal Telecommunications Law. Retrieved on 7th September, 2011 from http://www.law.cornell.edu/supct/html/00-511.ZO.html

[12] Kiessling T. & Blondeel Y. (1998). The EU Regulatory Framework in Telecommunications -A Critical Analysis, Telecommunications Policy, retrieved on 28th August, 2011 from http://www.uni-konstanz.de/FuF/VSRW_TPCh20.pdf

[13] Kabay M. E. (2008). A brief History of Computer Crime. Retrieved on 9th September, 2011 from www.mekabay.com/overviews/history.pdf

[14] Lehr W & Kiessling T. (1999). Telecom regulation in the US and the European Union: The Case for Centralized Authority in Competition, Regulation and Convergence: Trends in Telecommunications Policy Research. Lawrence Erlbaum Associates, Mahwah, NJ. Retrieved on 20th August,2011 from http://people.csail.mit.edu/wlehr/Lehr-Papers_files/LehrKiesslingTPRCVolume.PDF

[15] Monzur K (2009). GSM Network Architecture. Retrieved on 11th August, 2011 from http://www.pdfszone.com/pdf/gsm-architecture.html

[16] MTN Student Guide (2010), Network Architecture retrieved on 31st August, 2011

[17] Roelofsen G. (2000). TETRA Security-, Information Security Technical Report, Elsevier Science, Volume 5 (3), pp 44-54.

Retrieved on 12th October, 2011 from http://www.ida.liu.se/~g-johsi/docs/ecwi10_sigholm.pdf

[18] Theo, D. & Staffan, H. (2007). A brief History of Mobile Telecommunication in Europe. Journal of Telematics and Informatics. Vol. 24(3). Retrieved on 11th August, 2011 from http://dl.acm.org/citation.cfm?id=1265998.1266276&coll=DL&dl=GUIDE&CFID=63789688&CFTOKEN=45728926