Automatic Monitoring & Detection System (AMDS) for Grey Traffic

Mahmood A. Khan, Syed Yasir Imtiaz, Mustafa Shakir

Abstract— **International incoming grey traffic is currently one of the most important issues for both the Regulator and legal telecommunication operators in Pakistan. The major reason for higher grey traffic in Pakistan is because of international settlement rates which are higher than the cost of domestic termination rate. The grey traffic operators gain financial advantage by offering low international incoming termination rate to international carriers and thus bypass the legally established telecom network. In this paper, a detailed overview of grey route along with its termination techniques is discussed. Some of the existing techniques for monitoring and detection of grey traffic are compared and a novel method is proposed using the flow level characteristics of network traffic that will be more efficient and accurate for monitoring and detection of Grey traffic.**

Index Terms—**Grey traffic monitoring, Grey traffic detection, Network Security, Legal & ethical issues**

I. Introduction

THE world has become a global village due to inter-connectivity of different types of communication networks around the world. These communication networks are easily accessible but at the same time vulnerable to security risks. The telecommunication networks are managed by different Telco's, however; these telco's are supervised and controlled by regulatory authorities. The companies also pay taxes to the government from their profits. The use of Grey traffic in communication network affects not only the telco's but also the government.

Grey Traffic is a term used for illegal termination of international communication traffic in any country. The communication done via defined routes is termed as legal but if it is routed through un-defined routes is grey traffic. These few entities providing communication through illegal routes cause revenue loss to the telecom companies as well as the Government.

For example, telecom traffic originating from United States of America (USA) is transmitted via Internet Protocol (IP) to Voice over Internet Protocol (VoIP) [1] routers in Pakistan and from there, it is terminated to local Pakistani Public Switch Telephone Network (PSTN) via Wireless Local Loop (WLL) and local mobile numbers. This whole process is "white" from USA's perspective but is "black" from Pakistan prospective. In general, there are three types of routes that are used in communication networks:

- **White Route:** both source and destination have legal termination.
- **Black Route:** both source and destination have illegal termination.
- **Grey Route:** the termination is legal for one entity or country, but illegal for the other end.

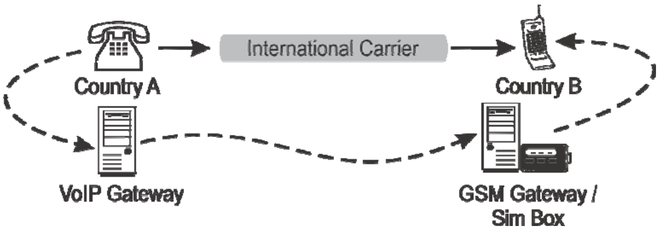

Fig 1: Grey traffic routing

This research paper focuses on the influence of Grey Traffic in the Telecom sector of Pakistan. We have analysed the existing technologies used around the world and then proposed a solution named "Automatic Monitoring and Detection System (AMDS) for Grey Traffic". AMDS will be installed at the main gateway exchange where all the communication traffic is routed; in our case, it is Pakistan Internet Exchange (PIE). AMDS is able to collect and analyse large volumes of data from several sources and deliver effective solution to cater the revenue loss caused by Grey Traffic. The main objectives of this solution are:

- To develop an independent and automatic system that monitors and detects grey traffic on Telco's network to assure national security.
- To contribute to local and international Telecom industry by supplying a vendor independent solution for detection of grey traffic that could compete with the international market of similar products.
- To develop a novel algorithm that acquires real-time CDRs (binary files) by interfacing to WAN at Telco's site and further store them to large database for analysis.
- To develop application software (KPI Engine) that analyzes the stored data (CDRs) and detect grey traffic by using specified parameters.

Manuscript received June 19, 2015; revised July 23, 2015. This work was funded by the National ICT R&D Fund working under Ministry of IT & Telecom: Grant ICTRDF/TR&D/2012/22.

M. A. Khan is the Director of Center for Advanced Studies in Telecommunication (CAST), COMSATS Institute of Information Technology, Islamabad, Pakistan (corresponding author to provide phone: +92-51-9049250; e-mail: mahmoodashraf@comsats.edu.pk).

S. Y. Imtiaz is an Assistant Professor at Center for Advanced Studies in Telecommunication (CAST), COMSATS Institute of Information Technology, Islamabad, Pakistan (e-mail: yasir_imtiaz@comsats.edu.pk).

M. Shakir is an Assistant Professor at the Department of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad, Pakistan (e-mail: mustafa.shakir@comsats.edu.pk).

II. Literature Review

A. *Grey Traffic Detection*

There are several methods of identifying grey traffic [2]. Previously, the communication traffic was identified on the basis of signatures of payloads or port numbers in packet headers, but that technique was unable to provide precise results because these elements can be changed or masked by the applications or likely to vary with the arrival of newer versions. Therefore, in this paper an effective detection technique is proposed which is based on flow-level characteristics of the traffic such as packet rate, packet length and inter-arrival time etc. As these features cannot be changed by applications, therefore, it is ought to be more effective in VoIP detection process.

On the basis of our developed solution, the Grey routes can easily be detected by heavy loads in certain network areas or incomplete call information or short voice calls. In case of heavy load on network, the Grey Traffic can be detected by three methods which include:

- Mobile phones (or Global System for Mobile (GSM) Gateway) termination that cause heavy loads on local mobile phone exchanges
- Media Gateway (MGW) in IP backbone termination that cause heavy load on MGW and soft switch
- Subscriber Access Line termination that cause heavy load in local telephone exchange

Calls that are routed by using Grey Route often lack the complete call information like originating source number, bearer service information etc.; so such call can be considered as grey traffic. Short voice calls are another sign of grey traffic that are caused by the repetitive dialling by the customer to get better voice quality.

1) *Approaches used to address grey traffic*

Mainly two approaches are used to address the grey traffic problem i.e. future fraud (fraud that has not yet occurred) and ongoing fraud (fraud that is in process, meaning that the fraudulent call has already been connected).

a) *Preventing "Future" Fraud*

To prevent future fraud situation from occurring, mainly two approaches are used:

- Modifying the individual network elements configurations (i.e. databases, exchanges etc.) so that they restrict some fraudulent users from utilizing the network resources. This approach is difficult to implement as it only provide variable degrees of control.
- Relying on other operators to block fraud that is being generated on their network. By using this approach, a carrier has no real control over the outcome. Furthermore, there is also a chance that inter-carrier fraud prevention does not rank high enough on other operator's priorities list.

b) *Controlling "Ongoing" Fraud*

In this approach, when an ongoing fraudulent call has been identified by lawful interception [3], an "in-band" blocking method is used where noise or silence is injected in the call with the help of a probe so that the calling parties release the ongoing call, and further loss is avoided. Although this method can save further loss but it has following drawbacks:

- Costly as it needs probe coverage to every available T1/E1 link.
- Alerts the calling parties that someone is controlling the call.
- Does not disconnect the call itself but requires the parties to release the call.

B. *Existing Technologies*

Different companies around the world have been working to tackle the grey telephony problem. Almost all of them focus to rectify the grey traffic that is being operated through SimBox.

The mechanism behind Sevis system [4], a global provider of signalling solutions to network operators and telecom equipment manufacturers, is based on its signalling Application and Service Engine (ASE) platform, a standard-based carrier-grade SS7/C7 network mode that functions as an application and service engine. The technique behind this method is platform transparent which eliminates the complexity of a network. Basically standardized industry interfaces are used to allow the operator to correctly bill the terminating traffic maintaining network efficiency and call quality.

The Teralight Prevail Application [5] provided by Teralight Limited is another useful product for detecting Grey Traffic. The Prevail application is an integrated fraud-detection application that can detect and track down fraudulent traffic in real-time. The basic design behind the application is a real-time monitoring of all the data from the Caller ID Box in forms of Call Detail Records (CDRs) and then process them to generate the required reports in real-time.

Mocean Subscriber Identity Module (SIM) Box Detector [7] is another effective method of detecting grey traffic by providing a tracking Caller Line Identification (CLI) to facilitate mobile operators for monitoring of international calls on international mobile networks.

The Cibertec's Bypass Detection System [6] is based on the inspection of international calls to the customer networks in a country. This application comprises remote traffic generator, target frame, irregular traffic report server and user/supervisor support services.

Although many companies have presented solutions to tackle grey traffic, but most of these are designed to detect grey traffic through SIM Boxes only. There are many other ways for the occurrence of gray traffic e.g. through VoIP Gateways. Since the proposed solution is designed for the higher hierarchy therefore it will cover all the gateway bypass methods including these two, which implies that it will be a complete solution; not limited to only SiMBOX or VoIP generated grey traffic.

III. Grey Traffic in Pakistan

According to Pakistan Telecommunication Authority (PTA), Grey telephony is defined as: [8] [9]

"The use of illegal gateway exchanges to bypass legal Pakistan Telecommunication Company Limited (PTCL) gateways and terminate/originate international traffic, including through VoIP gateways, GSM gateways, WLL phones, mobile SIM or other related equipment so as to avoid applicable taxes and/or regulatory fee"

The telecommunication market of Pakistan was an exponentially growing market during the last decade. With the emergence of IP Based applications and technologies, telecommunication market has been revolutionized but at the same time, it has given rise to VoIP traffic which bypasses the legal communication gateways or switches. This process spoofs the voice traffic into the country and makes it appear as locally originated traffic. The illegal routes make it possible for the companies to offer reduced call rate as compared to the actual telecom operator tariff. In addition to this, grey calls will cost less than normal white route calls for obvious reasons as they don't provide full services to the end user. They have certain drawbacks like bad voice quality, low call completion rate, congested network calls, no call receiving for inbound roamers and no proper access of network services by outbound roamers.

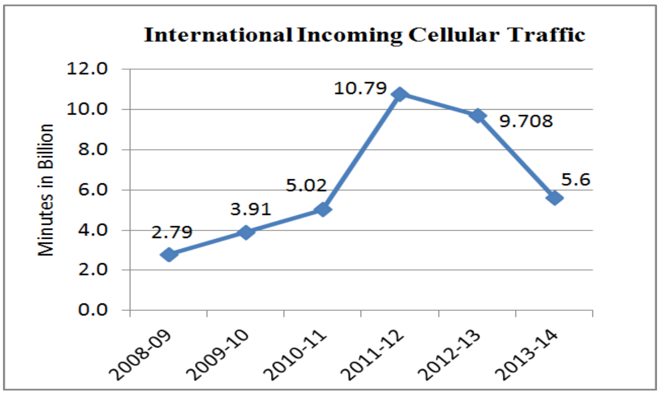

Fig 2: International incoming cellular traffic in Pakistan [10]

The telecom sector has grown enormously which is depicted in fig 2. This growth has caused a severe competition between telecom Operators to reduce their tariff which affected their profit. Under such conditions, this cumulative loss is further enhanced by the usage of Grey Telephony. Grey Traffic also cause a security risk as, it cannot be monitored directly. Therefore, there is a strong requirement of a system that may enable the Government to detect grey traffic. Generally, the grey traffic is initiated by small entities through VOIP routers setup in homes and offices throughout Pakistan. Due to this grey traffic (which is estimated about 13.3 million minutes per day or more than 50% of total international traffic entering the country) it is estimated that the Government faces a loss of over $35M per annum [11].

A. Measures Taken By PTA to Control Grey Traffic

PTA is continuously engaged to control grey traffic. On one side, it has taken forced measures to control the illegal use of gateway exchanges to originate/terminate international traffic through GSM Gateways, WLL Phones, VoIP gateways and mobile SIMs. On the other side, it has also taken both technical and regulatory measures which helped in reducing grey traffic.

PTA imposed a financial premium called as Approved Settlement Rate (ASR) on Mobile cellular operators for every international call. ASR comprises of Access Promotion Contribution (APC) and Long Distance and International (LDI) operator share. During the past couple of years, PTA has collected around $400 Million against APC for Universal Service Fund (USF) to promote services and utilize infrastructure in rural areas where telecom services are unavailable.

Recently, the government has taken a step towards elimination of grey traffic by withdrawing the controversial International Clearing House (ICH) policy which has brought the APC to zero. Due to the implementation of this policy, call rates for international incoming calls to Pakistan are likely to go down which will result a significant decline in grey traffic [12].

IV. Working of AMDS

Our developed solution of Automatic Monitoring and Detection System (AMDS) functions as a real-time mediation platform to facilitate a large number of VoIP data requests. The AMDS will be able to provide information of where and how much grey traffic is being channelled. As far as the blocking of grey traffic is concerned, the traditional methods will be relied upon. This implies human intervention will be required in the form of help from Police, Federal Investigation Agency (FIA) or any other law enforcement agency as per PTA requirement.

A. AMDS Building Blocks

The building blocks of AMDS are depicted in fig 3. It consists of CDR collection block to collect data, CDR analysis and mediation block where collected CDRs are processed to generate analysis which are finally used by the reporting block known as Service Performance Reporting (SPR). The reports generated by the SPR are then used by the traffic management block in order to track and manage protocols and service level agreements to get best value reporting.

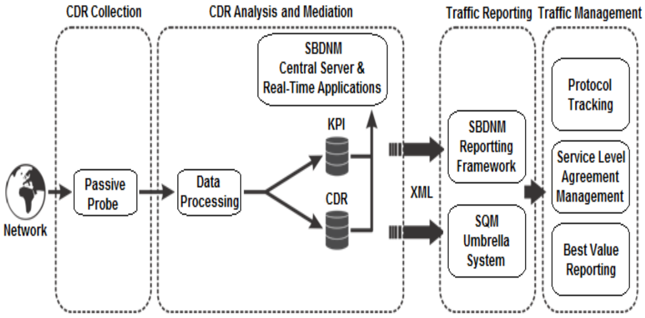

Fig 3: A detailed component diagram of AMDS

These blocks are further explained individually as follows.

1) CDR Collection

The key part of this solution is data capturing through Data Capturing Console (DCC). The DCC directly collect LIVE data in the form of Call Detail Records (CDRs) from the External Device/System, which is communicating through the Gateway. This CDR collection process is the responsibility of probes which can be active probes or passive probes depending on the mode of operation of the AMDS. When the system starts, the DCC starts receiving live data from the link in background on the main server. Data will be captured continuously through it and will be forwarded to the DB for storage in the Database. Due to huge live data capturing at this console, it necessary to forward this to DB engine. This CDR generator or mediation software has been developed with .net framework environment under J# support. This module produces records based on customer's usage profiles.

The probes are connected to WAN which consist of E1 links of all the operators connected to the Transit Exchange, NGN or a PIE (Pakistan Internet Exchange) in this case. For the first time, the AMDS needs to be trained through passive probes. Once the training of the AMDS is complete, active probes are deployed in real-time for grey traffic detection.

2) CDR Analysis and Mediation

Once the CDRs are collected, they need to be translated and analysed. The CDR Analysis and Mediation Block is responsible for the translation and mediation of collected data. The combined process of collection, validation, normalization and consolidation is referred to as mediation and is one of the most important blocks of AMDS. The main module of this block is Signalling Based Data Network Monitoring (SBDNM) system which will be responsible for capturing and managing of the signalling traffic that are later used for generation of reports by SPR for the traffic management and grey traffic detection. The Key Performance Indicator (KPI) tool/module will provide a comprehensive suite of technologies enabling businesses to monitor, visualize, and analyse signalling based data network. The system supports visual data mining of the data extracted and aggregated from signalling based data network and interactions with the application. Beyond the analysis of mediated/generated CDR, this system is unique because it provides all the data that is needed for testing a Telecom Information System component.

The binary/hex data, which is captured by the DCC, must contain all the data required such as Source IP, Destination IP, Source HW Address, Destination HW address, Protocols, Source Ports, Target Ports, Text message showing the details of the process etc. The above fields may be for further monitoring and detection purpose.

3) Traffic Reporting

This module inserts records into Databases in specific order where code is based on Multi-Threading technique. The whole record is being distributed into threads or small pieces of codes for fast system execution in microseconds. The technique helps to manage huge data in tera-bytes without providing extra load on the system or hanging the system.

Reporting is done in order to give the data a representation for a specific purpose. In this block, the Service Performance Reporting (SPR) module provides an independent end to end online and batch performance QoS reporting of networks.

This block is a User Interface to filter, display or export the required data into MS Excel or PDF file. System provides a front end Screen for Filtering criteria during specific dates selected by user. Based on these dates, system will display all the dates available in the system in a dropdown menu. User will select a date from this list for displaying data of that particular date.

- Source/ Destination IP Address
- Source/ Destination Hardware Address
- Source/ Destination Ports
- Protocols selection with the Check Boxes
- Any text string for Text data filtering

Since the Ports are thousands in number, an option has been given where user can enter multiple ports by separating them by commas. System will filter data based on all the ports entered by the user one by one. For protocols, system displays all protocols in the list found in the System data. User has the option to check one or multiple protocols. Another way is to select ‘AND’ option from the list that will filter data by combining the entire field’s data, entered by the user.

4) Traffic Management

The reports generated by the SPR module are used by the traffic management block for statistical review in order to track and manage protocols and service level agreements to get best value reporting. Some of these reports include:

- Circuit Switched Interconnect (CSI) statistical reports - contain all the required data to analyse service performance of calls passing through a network based on recommendations by the ITU (E.425) & ETSI (202 057)
- Answer Seizer Ratio and Network Efficiency Ratio reports - follow the industry standards E.422 & E.425 and are readily available for in-depth analysis. This analysis

easily identifies that which suppliers provide best service for a particular destination for call completion.

The report provides complete traffic record of calls in and out of the network used for production of quality of service reports, based on true and accurate traffic measurements.

V. Conclusion and Future Work

In today's world, the communication networks are the source of interconnectivity between different regions of the world. These networks are growing rapidly and more and more traffic is being routed between different sources and destinations per second. The communication through IP networks has provided opportunity to small organizations to come into the business and earn more with small investments. These organizations offer cheap rates on international traffic and by-pass the legal routes. This Grey traffic causes huge revenue loose to Telco's which effect government revenue in terms of taxes.

In this funded project, a technique has been developed for the detection of illegal network traffic termed as "Grey Traffic". Government of Pakistan has made a lot of efforts to control grey traffic, but as the technology is upgrading, the Grey Traffic Operators are also using latest techniques/tools to bypass the System. We have presented a system that accurately identify and detect grey traffic by using the flow level characteristics of network traffic rather than the signature of payloads and restrict it to save the loss in revenue.

In future, this AMDS can be integrated as main component of Fraud Management system. By further adding features of GIS, the system can locate the exact location of illegal international gateways and thus can enable the regulators to stop grey traffic efficiently.

References

[1] Idrees F. and Khan U. A.: "A Generic Technique for Voice over Internet Protocol (VoIP)," *International Journal of Computer Science and Network Security,* vol. 8, no. 2, pp. 52-59, 2008.

[2] Rasheed C. M. A., Khaliq A.: Sajid A. and Ajmal S., "Identification of Hidden VoIP (Grey Traffic)," *Journal of Computer Networks,* vol. 1, no. 2, pp. 15-27, 2013.

[3] Singh J. Kaur L. and Gupta S., "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks," *The International Arab Journal of Information Technology*, vol. 9, no. 3, pp 201-207, 2012.

[4] "Active Fraud Eliminator," Sevis Systems, [Online]. Available: http://www.sevis.com/root/pages/signaling_solutions/afe.shtml. [Accessed April 2015].

[5] "Bypass Fraud Detection Services," Teralight, [Online]. Available: http://www.teralight.com/bypass-fraud-detection-services.html?i=tnt-solution. [Accessed April 2015].

[6] "Bypass Detection," Cibertec Internacional, [Online]. Available: http://www.cibertec.com/serv-bypass-detection.php. [Accessed April 2015].

[7] "MOCEAN SIM Box Detector," Micro Ocean Technologies, [Online]. Available: http://www.mocean.com.my/SIM_box_detector_solution.php. [Accessed April 2015].

[8] Bhatti B., "Grey Telephony in Pakistan," TelecomPk.net, [Online]. Available: http://telecompk.net/2007/06/12/voip-grey-telephoney-pakistan/. [Accessed April 2015].

[9] PTA, "Annual Report 2011. [Online]. Available: http://www.pta.gov.pk/annual-reports/pta_ann_rep_11.pdf. [Accessed March 2015].

[10] PTA, "Annual Report 2013. [Online]. Available: http://www.pta.gov.pk/annual-reports/annreport2013_1.pdf. [Accessed March 2015].

[11] Baloch F., "Telecom: PTA's new system to curb grey traffic up and running," The Express Tribune, [Online]. Available: http://tribune.com.pk/story/627643/telecom-ptas-new-system-to-curb-grey-traffic-up-and-running/. [Accessed April 2015].

[12] Business Recorder, "Access Promotion Contribution made zero: Controversial ICH policy withdrawn," [Online]. Available: http://www.brecorder.com/taxation/181:pakistan/1193830:access-promotion-contribution-made-zero-controversial-ich-policy-withdrawn/. [Accessed May 2015].