Optimization of Revenue Assurance and Fraud Management System by designing new KPIs: case PTCL

Umar Mushtaq
Institute of Communication Technologies
NWFP University of Engineering & Technology,
Peshawar, Pakistan

Muhammad Khalil Shahid
Institute of Communication Technologies
NWFP University of Engineering & Technology,
Peshawar, Pakistan

ABSTRACT
With increasing company dependence upon Revenue Assurance and Fraud Management (RAFM) processes and the rising complexities in sustaining an efficient RAFM structure, companies require a greater focus upon improving and integrating new elements into existing RAFM dynamics. Telecommunication companies are some of the most vulnerable businesses in the world when it comes to fraud and they are profound to ensure that all of its RAFM activities and processes are managed in a centralized fashion to ensure a complete end-to-end acuity across the organization. The main objectives of this paper are: Analysis of existing Key Performance Indicators (KPIs) of RAFM system, Identification of sources of revenue leakages and frauds in existing RAFM system and Designing of new KPI for optimizing RAFM system. This research will assist to improve RAFM practices and processes in order to guarantee that all revenues and profits are optimized for the business and the maximum value is delivered.

1. INTRODUCTION
Revenue Assurance is the procedure that a telecom operator uses to ensure that all revenues due for the services provided to customers and 3rd parties are accurately billed, accounted for and completely collected whereas handling fraud to an acceptable level [1]. Revenue assurance is the umbrella term that describes the activities that a telecommunications company will start in order to ensure that their processes and procedures curtail revenue leakage. This leakage occurs when revenue that has been earned by the company, such as when services are rendered to the customer, but lost on its way to the billing systems so that the customer never gets debited.

Telecommunications fraud, already a major threat in currently focused networks for voice and data traffic, is anticipated to increase in upcoming converged networks referred to as Next-Generation Networks (NGNs). Due to some of their key features, such as being based on the Internet Protocol, NGNs create new challenges for operative fraud detection [2]. Fraud Management is the analysis and a set of tools to provide analysis, control and monitoring over the end-to-end revenue stream processes. It permits early disclosure of revenue leakage or undue costs and their recovery. Revenue Assurance is not just about finding leakage. It is a discipline that discloses weaknesses in operating support systems, processes, structure, and business strategy that sources revenue leakage or excessive costs [4].

The purpose is to establish a signaling monitoring system that should collect, co-relate, store and process control layer data i.e. signaling protocol data units (PDUs) from the following Pakistan Telecommunication Company Limited (PTCL) platforms: Public Switched Telephone Network (PSTN) Switches, Wireless Local Loop (WLL) Mobile Switching Centers (MSCs), WLL Next Generation Networks (NGNs), C-4 NGN, C-5 NGN, PRI exchanges, Internet Gateways (PIE network). Protocols that have been monitored & processed are Signaling System no. 7 (SS7) including ISDN user part (ISUP) and Intelligent Network Application Protocol (INAP), SIGTRAN (Message Transfer Part 2 User Adaptation Layer - M2UA, Message Transfer Part 2 Peer-to-Peer Adaptation Layer - M2PA, Message Transfer Part 3 User Adaptation Layer - M3UA), Session Initiation Protocol (SIP-T, SIP-I), Media Gateway Control Protocol (MGCP), H.323 and H.248.

2. LITERATURE REVIEW
Fraud Management and Revenue Assurance (RA) are both substantial factors in upholding operators margins, and with the growth in complication of networks and services and with the increasingly developed use of technology by fraudsters, these functions require an end-to-end policy. Internet telephony compromises the typical telephony services. However, the changeover to Internet based telephony services also provides an opportunity to create new services more rapidly and with lower convolution than in the prevailing public switched telephone network (PSTN). The Session Initiation Protocol (SIP) is a signaling protocol that creates, modifies and terminates links between Internet end systems, including conferences and point-to-point calls [5].

Signaling System Number 7 is the protocol used by the telephone companies for interoffice signaling. In the past, in-band signaling techniques were used on interoffice trunks. This process of signaling used the same physical path for both the call-control signaling and the actual connected call. This method of signaling is unproductive and is rapidly being replaced by out-of-band or common-channel signaling techniques. SS7 has gradually becomes the backbone of today's communication network. It performs out-of-band signaling in support of the call-establishment, billing, routing, and information-exchange functions of the PSTN. In order to flawlessly integrate the IP network with the PSTN, it is important to retain the SS7 information (ISUP) at the points of inter-connection and use this information for the purpose of call establishment [8]. SIGTRAN protocol is for the backhauling of SS7 and M2U User signaling messages over IP using the Stream Control Transmission Protocol (SCTP). The SIGTRAN protocol stack consists of 3 components: A standard IP layer, Stream Control Transmission Protocol and Adaptation layer with M2PA, M2UA, M3UA, and SUA

protocols. SIGTRAN would be used between a Signaling Gateway (SG) and Media Gateway Controller (MGC). It is estimated that the SG receives SS7 signaling over a standard SS7 interface using the SS7 Message Transfer Part to provide transport.

The Signaling Gateway would act as a Signaling Link Terminal [11]. It also supports the transport of Signaling System Number 7 Message Transfer Part Level 3 signaling messages over Internet Protocol using the services of the Stream Control Transmission Protocol. This protocol would be used between SS7 Signaling Points using the MTP Level 3 protocol. The SS7 Signaling Points may also use standard SS7 links using the SS7 MTP Level 2 to provide transport of MTP Level 3 signaling messages. The protocol operates in a manner similar to MTP Level 2 so as to provide peer-to-peer communication between SS7 endpoints [13].

The Session Initiation Protocol (SIP) is an application level signaling protocol for setting up, modifying, and terminating real-time sessions between participants over an IP data network. SIP can support any type of single-media or multi-media session, including teleconferencing. The Session Initiation Protocol (SIP) is deliberated as a powerful alternative to H.323 in the prevailing Voice over IP (VoIP) signaling system in the future [8].

The Session Initiation Protocol (SIP) is a client/server protocol used for the initiation and management of communications sessions between users. SIP end systems are called user agents, and intermediate elements are known as proxy servers [14].

Elements of SIP call flows include SIP User Agents and Clients, SIP Proxy and Redirect Servers, and Gateways to the PSTN (Public Switch Telephone Network). IP telephony scenarios include SIP Registration, SIP to SIP calling, SIP to Gateway, Gateway to SIP, and Gateway to Gateway via SIP. PSTN telephony protocols are exemplified using ISDN (Integrated Services Digital Network), ANSI ISUP (ISDN User Part), and FGB (Feature Group B) circuit associated signaling. PSTN calls are demonstrated using global telephone numbers from the PSTN and private extensions served on by a PBX.

3. METHODOLOGY

Making changes to signaling networks is a task of great obligation, considering the large increase in traffic volume and the fact that traffic-carrying networks rely heavily on smooth signaling. Deviations that are not correctly made may even cause these networks to go out of service. The need for changes is created by a number of trends: digitization of exchanges, reconfigurations of connections, and the introduction of new nodes for IN etc. The number of signaling points in the network is increasing, thus increasing network complexity and threat of introducing faults.

ZTE's signaling monitoring platform which is named as ZXT2000 monitoring system can detect the running status and quality of signal network and implement analysis and maintenance to the service network. ZXT2000 is an entire net, flexible and open signal capturing, processing and analyzing system. It's an important technical method for management and maintenance of signal network. Simultaneously, the system can provide comprehensive data support and accurate data confirmation for the third system, and provide strategy support for the service management, monitoring and analyzing of service quality, charging and settlement, planning of network, analyzing of service execution.

ZXT2000 monitoring system implements the collection, analysis and processing for the Signaling Transfer Protocol (STP) through the following functions: Collection and storage of binary code stream with delimitation of MSU message, Protocol analysis of MSU message with synthesis of call record/event, Centralized storage and pretreatment of calling detail records / transaction detail records CDR/TDR records, Service analysis and monitoring based on CDR/TDR records.

ZXT2000 Capturing Layer is composed of the major parts of front processor (Probe), high-impedance insulator & Digital exchange controller (DXC). The signaling probe accepts the switch product architecture allowing hot-swapping, high reliability, high stability, high accuracy, low power consumption and low noise. This layer makes the system access signaling links, collects raw signaling messages, synthesizes the raw signaling messages into CDR or TDR, and then transfers them to next layer. The signaling monitoring platform is connected with the signaling system in high-impedance isolator bridge connection mode.

The system features extreme security performance. The platform collects the signaling messages through the high-impedance isolator on the digital distribution frame (DDF) where the E1 trunk is located and prevents signal reversion, thereby collecting signaling data. The high-impedance isolator connects to SS7 links though high-impedance technology ensures no signal sending-back under any condition, providing high-security for SS7 network. The DXC digital cross connection equipment converge the 64K links in multiple E1s into one E1, increasing the utilization of the transmission resource and at the same time, it also has the signal amplification function for long distance transmission after high-impedance isolator bridged.

ZXT2000 Processing Layer is composed of the major parts of front-end server and database server. The front-end server preprocesses the data, calculates network load and sends alarm to operational and maintenance terminals; the database server acts as a data platform, responding for operational command and give the result to the operator. This part implements the following functions: CDR processing, basic statistics processing, Alarm processing, Application Layer. ZXT2000 monitors the signaling network in real time, generating the CDR records and service analyzing various protocols like SIP, ISUP, SIGTRAN, H232 and H248.

With the statistics pre-processing of the front-end application server, the data is categorized and saved in the database. For the data in the database, it uses the database technology to analyze and query various service statistics i.e. generating reports based on the above protocols. It supports the graphical analysis, detail query, saving and printing functions by applying formulas. It also provides the function of displaying the indexes graphically in real time.

ZXT2000 is used for collecting signaling information on physical links. The ZXT2000 data collection platform features: High-speed collection and distributive forwarding through Ethernet switching, Improved data collection and processing capabilities, Collection of E1, IP, ATM, and IMA signaling information and expansion of physical interfaces, Flexible configuration supporting mix-insertion of various signaling collection boards, Flexible configuration of IP addresses of boards, Hot-swapping of boards, Hardware complying with lead-free standards, Flexible configuration of clock synchronization modes, including precise GPS mode and convenient NTP mode, Professional network management

software to implement remote diagnosis, troubleshooting, and online upgrade of interface modules.

Following KPI's of ZXT2000 RAFM system have been analyzed in detail:-

- **Heavy Caller**

  Call count is big against Origination Number, i.e. a large number of calls connected from one number

- **Heavy Called**

  Call count is big against Destination Number, i.e. a large number of calls received on one number

- **Traffic Comparison**

  Outgoing call Counts from Origination point should be equal to Incoming call Counts at Destination point

- **Trend Analysis Destination**

  Call trends at Destination point verified, i.e. call trends checked on different dates

- **Trend Analysis from source**

  Call trends from Origination point verified, i.e. call trends checked on different dates

- **Heavy Calling (Grey SIM Box)**

  International calls bypassing from Origination point, i.e. detecting the grey trafficking

- **Call Count as Source and Destination**

  Incoming and Outgoing call Counts at one point, i.e. both should be same for single source/destination

- **Call Leg Analysis (Call Trace Analysis)**

  Legs between source and destination should be appropriate, i.e. there should be single leg between 2 local numbers

  Sources of revenue leakages and frauds have been detected after detailed research of call records regarding each KPI.

After analysis of above KPIs and their minor deficiencies, a following new KPI has been designed which checks the outgoing and incoming call counts on a particular source exchange point.

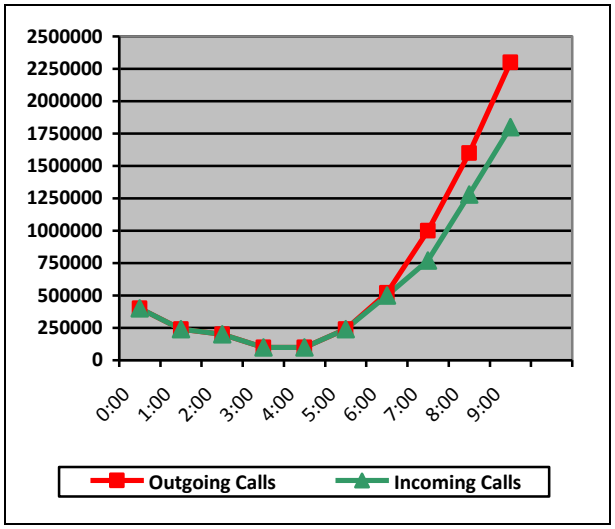

Fig.1 - Duration based Call analysis

* Large outgoing count as compared to incoming count depicts a fraud at this exchange point. The pointed Destination Exchanges need to be checked for fraud.

4. CONCLUSION AND RECOMMENDATIONS

With each transitory year, and with the increasing telecommunication evolution, the need of the revenue assurance system grows. Revenue management systems, while improving with each generation, are still a long way from keeping up with the existing growth. Revenue leakage will continue to increase due to the vibrant telecom environment; however, if companies can implement a successful revenue assurance program, any revenues found internally will have an abrupt impact on bottom line numbers. If not, Telco's will be throwing away shareholders' money and investors will price this risk into valuations or will move elsewhere. Operators should make sure they are setting the right, flexible technology to cope with current and future business and technological requirements in order to compete and survive into the future.

ZXT2000 has been widely adopted by telecom carriers, effectively ensuring operation stability in communication networks. Network monitoring is increasingly deployed in more fields and delivering more functions along with development of new communication technologies. A successful RAFM KPI should align many corporate processes that impact the revenue stream and integrate the underlying business support and operational support systems.

As stated in preceding paragraph KPIs, there are a lot more from which frauds and revenue leakages can be determined. To conclude it can be said that all the mentioned KPIs and the new proposed KPI help to identify the revenue leakages and frauds. The signaling monitoring equipment need to work efficiently providing its full performance as measurement of each KPI is dependent on integration of all modules for data capturing. Thus, careful analysis of each KPI is very important to check each fraud on all levels.

Practical Amplification: This research study will make a significant contribution on the frauds & revenue leakage sources in PTCL network. This will help and guide the management to know the basic problems of frauds being faced by the organization and will increase the power of decision and judgment.

Limitations: Yet this research has a claim to perfection, there are some limitations too regarding to this research. We have data availability issue in terms of KPI reports as we cannot get more data for analysis due to private/personal call records. There seems to be no comprehensive feasibility study on fraud management and revenue assurance as most research papers only target few particular applications. Data gathering has been difficult as most of the information had to be sourced from PTCL's live network.

5. REFERENCES

[1] Jogesh Patel, 2006, "Analysis and Modeling of Fraud and Revenue Assurance Threats in Future Telecommunications Network & Service Environments"

[2] Bihina Bella M.A., M.S. Olivier M.S., Eloff J.H.P., 2005, "A fraud detection model for Next Generation Networks", Southern African Telecommunication Networks and Applications Conference (SATNAC)

[3] Rob Mattison, 2005, "The Telco Revenue Assurance Handbook", XiT Press, Illinois, USA

[4] Alison L, Shelia H, Michael C, 2004, "Revenue Assurance Telecommunications Management Forum", IBM Business Consulting Services

[5] Schulzrinne H., Rosenberg J., 1998, "Signaling for Internet Telephony", Technical Report CUCS 005-98, Columbia University, New York.

[6] Saharon Rosset, Uzi Murad, Einat Neumann, Yizhak Idan and dGadi Pinkas, 1999, "Discovery of Fraud Rules for Telecommunications", KDD '99 Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining

[7] Sangwon Min, 1934, "SS7 and Sigtran Architecture", Communication Protocol Engineering Lab Kwangwoon University

[8] Zhang Yuan, 2002, "SIP-Based VoIP Network And Its Interworking With The PSTN", Electronics & Communication Engineering Journal (Volume:14 , Issue: 6)

[9] Arango M., Dugan A., Huitema C., Pickett S., 1999, "Media Gateway Control Protocol (MGCP)", Network Working Group – October

[10] Schulzrinne H., Rao A., and Lanphier R., 1998, "Real time streaming protocol (RTSP)," RFC 2326, IETF – April, ITU-T Work Programme : J.703

[11] Morneault, K., Pastor-Balbas J., 2006, "Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)", Network Working Group, The Internet Society (2006)

[12] Morneault, K., Dantu, R., Sidebottom, G., Bidulock, B., and Heitz J., 2002, "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer", RFC 3331

[13] George, T., Bidulock, B., Dantu, R., Schwarzbauer, H., and K. Morneault, "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Peer-to-Peer Adaptation Layer (M2PA)"x`

[14] H. Schulzrinne and J. Rosenberg, 2001, "SIP: Session initiation protocol – locating SIP servers," Internet Draft, Internet Engineering Task Force, March

[15] Johnston, S. Donovan, R. Sparks, C. Cunningham, D. Willis, J. Rosenberg, K. Summers, and H. Schulzrinne, 2001, "SIP call flow examples" Internet Draft, Internet Engineering Task Force, April

[16] Handley M., Schulzrinne H., Schooler E., Rosenberg J., 1999, "SIP: Session Initiation Protocol", Network Working Group - March

[17] Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M., Schoolar E., 2002, "SIP: Session Initiation Protocol", Network Working Group - June

[18] Mahy R., Biggs B., Dean R., 2004, "SIP: Session Initiation Protocol", Network Working Group - February

[19] Burger E., Spitzer A., 2005, "Basic Network Media Services with SIP", Network Working Group – December

[20] Mahy R., Sparks R., Rosenberg J., Petrie D., Johnston A., 2010 "A Call Control and Multi-Party Usage Framework for the Session Initiation Protocol (SIP)", Internet Engineering Task Force - May

[21] Rosenberg J., Schulzrinne H., Kyzivat P., "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)", Network Working Group – August

[22] Roach A. B., 2002, "Session Initiation Protocol (SIP)-Specific Event Notification", Network Working Group – June

[23] Brennen Reynolds, Dipak Ghosal, 2003, "SecureIP Telephony using Multi-layered Protection",

[24] Karl-Johan Grinnemo, Anna B., 2013, "Performance of SCTP-controlled Failovers in M3UA-based SIGTRAN Networks"

[25] Karl-Johan Grinnemo, Anna B., 2005, "Impact of Traffic Load on SCTP Failovers in SIGTRAN", ICN'05 Proceedings of the 4th international conference on Networking - Volume Part I