Paper: ASAT-14-088-CM

14th International Conference on
AEROSPACE SCIENCES & AVIATION TECHNOLOGY,
ASAT - 14 – May 24 - 26, 2011, Email: asat@mtc.edu.eg
Military Technical College, Kobry Elkobbah, Cairo, Egypt
Tel: +(202) 24025292 –24036138, Fax: +(202) 22621908

Performance Evaluation of Key Cellular Networks Operations Using Signaling Networks Protocol Analysis

Kh.Y. Youssef*, A.A. Zekri†

Abstract: The current communications world is characterized by increasing number of end user terminals, as well as the emerging convergence of different communication services with the IP world. Thus, keeping a good network performance across all domains within a heterogeneous network became a challenge. Accordingly, the complexity of the performance measurement mechanism became higher and is in a real need to simplification and accuracy to keep pace with the overwhelming growth. This paper deals with an approach of using the signaling networks protocol analysis in assessment of networks performance including the legacy core segment, the IP core segment, the wireless segment, as well as the application segment. As well, the use of the technique in the early detection of security attacks is elaborated which is based on network abnormal events detection A full analysis methodology is proposed, using statistical algorithms and mathematical modeling of a sample of traffic scenarios. As a conclusion, the proposed mechanism helps in simplification, quickness, and accuracy of measurements regardless of the manufacturer proprietary applications, and nodes architectures.

Keywords: Signaling, SS7, QoS, performance evaluation, network monitoring, network management, GSM, 3G, UMTS, security, eavesdropping.

1. Introduction

Telecom companies often focus on the Operation Management Centers (OMC) that is relying mainly on network nodes several counters to provide the central office with the most important data about network quality. Examples are counters for the number of incoming or outgoing handovers; call drops before, during, and after assignment; and dropped calls due to missing network or radio resources. The major advantage of measurements via the OMC is that it provides results about the quality of the entire network rather than a single node.

However, on the other hand, this level of information provided by the OMC is not enough to give a complete analyzable view about the network especially with the networks trend towards All-IP heterogeneous networks and IP convergence concepts that in turn add a lot of load on the shoulders of network operators to define and maintain a unified quality measures as well as protecting their networks against abnormal subscribers behaviors including aggressive use of network resources, unbalanced loads, congestions, as well as attacks.

* MEA Manager, Strategic Industries Research, Alcatel-Lucent.
† Professor of Electronics and Communications, Faculty of Engineering, Ain Shams University.

The objective of this paper is to propose algorithms that can be used for monitoring the wireless and mobile networks Quality of Service (QoS) and detection of predefined events in those systems based on the approach where the information contained in signaling networks layer is captured and encapsulated in the form of transaction detailed records (XDR). The collected XDRs are then subjected to post processing and post-analysis using statistical modeling techniques for improvement the accuracy of the results. For XDR we mean the Call Detail Records (CDR) for conventional calls, or the Packet Detail Record (PDR) for IP networks and media networks as IPTV, and TDR for network management transactions as mobility management location update, and handover traffic.

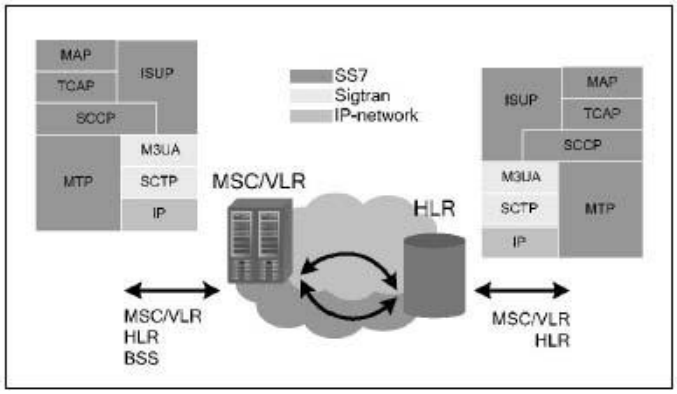

Fig. 1 Architecture of SS7/SIGTRAN network

Also, this algorithm helps in the detection of abnormal subscriber behaviors and anomalies as spam, security attacks, and network threats. In this paper, one example is presented to explain how this approach is beneficial together with the mathematical modeling to enhance the performance of cellular networks. As well, one practical case study is presented to highlight the volume of information signaling networks could provide.

2. Signaling Networks Overview

The signaling networks are historically used to setup and to clear Connections and or sessions between end users or machines, but nowadays its role is extended also for managing new applications and features of today networks technology. Among them is automated database access, in which telecommunications system call each other, and which are transparent to a caller, or the wide area of supplementary services , as GSM supplementary services. SS7 has become one of the most important assets within any carrier's network, already deemed important for interconnecting calls from one network to the next SS7 is a control protocol, used to provide instructions to the various elements within telephony network. These instructions may be how to route a call through the network, what features a caller has subscribed to, or, in the case of number portability, which carrier will be used to handle the call, or, in the case of mobile networks, which node handed over the attached subscriber. In order to provide this level of instructions, a great deal of information must be sent from an element to another.

Particular aspects of SS7 will continue to thrive throughout the signaling networks, but already the lower layers of the SS7 protocols are being replaced by protocols based on transmission control. SIGTRAN is the name given to an IETF working group that produces specifications for a family that provide reliable datagram service and user layer adaptation for SS7 and ISDN communications protocol. The most popular protocol defined by the SIGTRAN group was the stream control transmission protocol (SCTP), which is used to carry PSTN signaling over IP as in [7].

Several signaling protocols are used today and represent the signaling plan for all communication networks such as Media gateway control protocol, MGCP, a client-server protocol, used by telephony providers to control subscribers' requests, the Session Initiation Protocol (SIP) or H.323 that are peer-to-peer protocols. SIP was accepted as a 3GPP signaling protocol and permanent element of the IMS architecture. It is widely used as signaling protocol for Voice over IP, along with H.323 and others. H.323 is an umbrella recommendation from the ITU-T that defines the protocols to provide audio-visual communication sessions on any packet network. It is currently implemented by various Internet real-time applications, as NetMeeting. It is a part of the H.32x series of protocols which also address communications over ISDN, PSTN or SS7. H.323 is commonly used in Voice over IP (VoIP, Internet Telephony, or IP Telephony) and IP-based videoconferencing.

3. Signaling Traffic Monitoring Platform Overview

The data source of the quantifier parameters is selected to be the signaling layer between network nodes in both the mobile and fixed networks. Accordingly, the data acquisition technique is based on first, Selection of a proper signaling group, second, monitoring of all signaling links within the same signaling group, third, Capturing of signaling message according to the scope of measurement, fourth recognition and classification of signaling messages., fifth, decoding of the classified octets according to protocol standard identifiers for formulation of the XDR, sixth, mediation and cross correlation of related XDRs including multi-protocol and multi-leg correlation into one record to maintain consistency and integrity of the information, and removal of duplications. Finally, the final record is inserted into a central database management system.

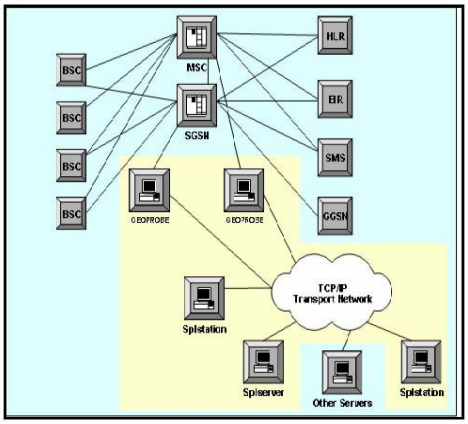

Fig. 2 Deployment of Tektronix probing system in the network

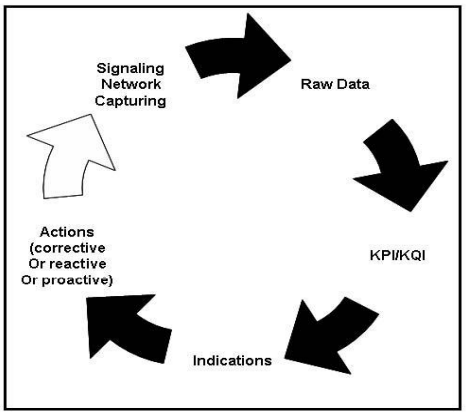

Fig. 3 Metrics Measurement Cycle

The acquisition system which is used for data capturing is Tektronix Geoprobe system which is a non-intrusive monitoring system. It provides data capturing and processing function on the signaling networks without incurring loss of performance or deterioration of service quality due to its passive monitoring theory of operation. The Geoprobe detects the signaling on the links between network nodes, and analyses this data to reconstruct the behavior of the network. By placing intelligent probes at sites of signaling concentration, the Geoprobe system can cost effectively piece together signaling from all the different links that relate to a single call or transaction. Geoprobe makes it possible to correlate signaling messages from different protocols and different switches that relate to a single call. The main advantages

behind the selection of this SS7 probe is attributed mainly to its vendor independence data integrity (high availability) and real time processing.

The Geoprobe system is composed of, Signaling MSU capturing unit (spIprobe) that contains application processor boards. The probe monitors traffic flow from selected links, collects signaling data, implements real-time distributed processing and call correlation. Administration Server (spIserver) which is a central administration point SUN server that stores configuration data for both the system and the Geoprobe system user, distributes alarms generated by the probes to users at the appropriate workstation and to external systems. It also hosts the ORACLE database server for local data storage. One application is developed to be the mediation processing platform and acts as the client entity for the database server is the mediation analysis Server used to transform the raw data that is captured by the probes into meaningful KPIs. The hardware platform of the analysis server is seized carefully to handle the traffic load that is expected to be incident on the server. The server specifications are dimensioned to be Special HP Quad-processor platform with 12 GB memory, and 300 GB high speed RAID disks.

4. Methodology of Signaling Event Detection and Classification

The mediation layer that is responsible for analysis of the XDRs and determination of faults criteria as service outage, or quality degradation is based on real time algorithm, as in [3]. The Real Time Algorithm (RTA) is based on the Renewal Theory [9],[10] applied *Type equation here.* to Bernoulli trials. To explain this, we will start to model the events of the system as random variables. For example, Let X be a random variable that represents an specific event in a Bernoulli experiment. The Sample Space of X can take two values

$$X = \begin{Bmatrix} 1 \\ 0 \end{Bmatrix}, \tag{1}$$

where the value X = 1 represents the occurrence of an specific event and 0 the occurrence of any other event. Let's also assume that the probability of X = 1 is equal to p. Now we introduce a new random variable Y which is the number of events occurring until a sequence of r ones is formed for the first time, as shown in Figure (4). According to the Renewal Theory, N = E(Y), the mean or the expected value of Y, can be given as

$$E(Y) = N = \frac{1-p^r}{p^r(1-p)} \tag{2}$$

Isolating variable r, we obtain

$$r = \frac{-\ln[N(1-p)+1]}{\ln p} \tag{3}$$

The value of r should always be rounded to the next integer number in order to assure that the probability of occurrence of a false positive alarm is restricted to a certain limits. Then, we should modify the last equation as

$$r = INT\left[\frac{-\ln[N(1-p)+1]}{\ln p}\right] \tag{4}$$

As a result, this last equation gives the number of times, r that an event should happen consecutively for the correspondent fault to be considered as having happened. The quantity is directly related to the probability p and the value N. N is directly related with the guarantee

that the false positive alarm will be generated in the stipulated limit. To analyze the relationship among these quantities, let's suppose, for example, that an event has an average of occurrence of 1% (p = 0.01) and that N is 100000, meaning one false positive alarm in 100000 alarms. Then, by entering with these values in (4) we obtain that r=3. Therefore, if there are 3 or more consecutive events the alarm will be generated. If we want to have a greater guarantee that the fault has occurred, that is, a lower probability of a false positive alarm, we must observe the corresponding event occurring a larger number of times in sequence. So, phenomena as intra-BSC handover failures for a certain switch will be considered only if the number of repetitions exceeds 3 in our case.

The algorithm is tested on normal CDRs from the OMC, as in [3] to analyze faults of various resources of the system, such as, Base Transceiver Station, RF channels, time slots, specific peripheral controllers, etc. Each time the QoS degrades the algorithm is applied in order to detect any anomalies. The detection of this type of failure is complex, considering that the generation of these problems is purely random. It will be easier and faster to detect it if there is some order in the degradation of resources. An order presumes smaller entropy or a greater amount of information than just purely random occurrences.

Another important variable that should be measured is the amount of time needed to detect the fault. We could observe that the algorithm's behavior related to time detection varies with the quality level as well as the quality of service (QoS) degradation level. We concluded that these algorithms are extremely efficient once there is a great degradation on the QoS of a resource. In these cases, the failure detection only takes a few seconds. When degradation isn't as critic, the algorithm may or may not detect the failure. Therefore, there's no way to guarantee the exact moment the degradation on the QoS will be detected.

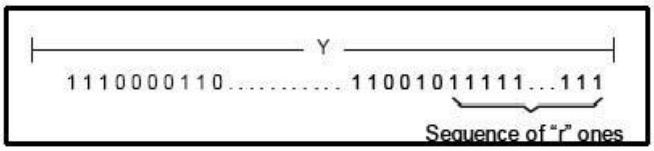

Fig. 4 Random Variable Sequence

5. Example, Applying Technique on Cellular Network Security Measures

5.1. Security Scenario Overview

Reference [4] proposed the eavesdropping security attack on mobile phones especially soft phones; the following scenario is presented in the reference as "Mary was curious about John's everyday life. She decided to eavesdrop on John through his mobile phone. She purchased a pair of "spy" mobile phones: a spying phone and a spied-on phone. She gave the spied-on phone to John as a birthday gift. When she wanted to eavesdrop on John, she used the spying phone to dial the number of the spied-on phone. Thus, the spied-on phone of John became a remote microphone through which Mary could hear all sounds around John when he was not using the spied-on phone for conversation. Based on the technique, we will describe later that John (the victim) is typically not spied on (overheard) when he is using the spied-on phone for conversation. Mobile telecommunication services have become very popular recently, and many people bring mobile phones with them wherever they go. However, we observe that mobile phones can be modified to become remote microphones for eavesdropping".

5.2. Projection of Scenario on Signaling Plane

To eavesdrop through a mobile phone, the software of the spied-on phone is modified to accommodate the eavesdropping procedure:

i. The eavesdropper dials the phone number of the spied-on phone. The IAM message is sent from the originating switch to the terminating MSC of the spied-on phone. The terminating BSS pages the called party.
ii. If the called party is in the radio's coverage, it sends the page response signal to the terminating BSS. The terminating MSC returns the ACM message to the originating switch. If the spied-on phone is not busy, a ringing signal is sent to the spied-on phone, and a ringback signal is sent to the spying phone.
iii. The spied-on phone obtains the caller ID from the ringing signal. It checks if the caller ID is the phone number of the spying phone. If not, the normal call setup procedure is performed. If the caller ID matches, the spied-on phone disables the ringing tone and turns off the speaker such that the victim is not alerted.
iv. Without having the victim to pick up the handset, the spied-on phone automatically turns on the transmitter (microphone) and sends an answer signal to the terminating MSC. The terminating MSC considers that the called party (the victim) has picked up the phone, and it sends the ANM message to the originating switch. The ringing tone is removed.

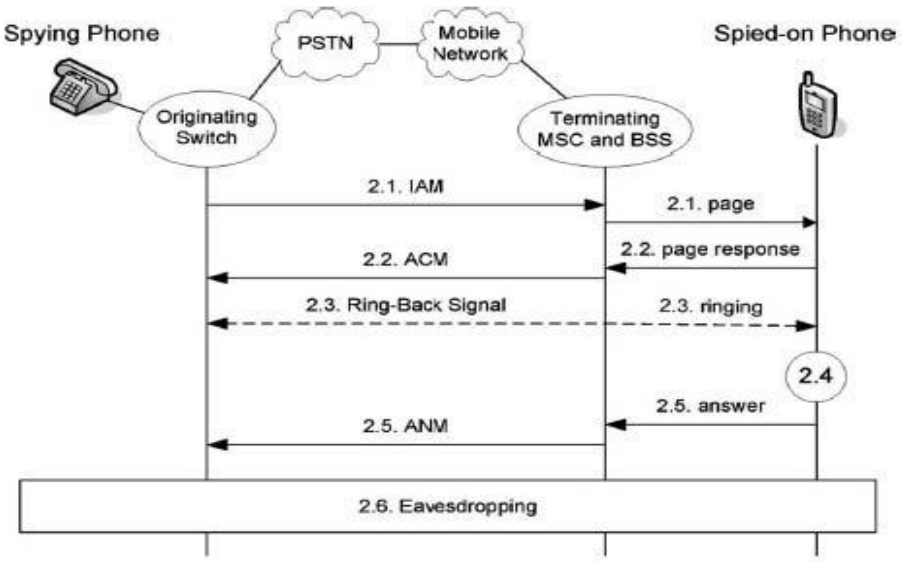

Fig. 5 SS7 signaling during eavesdropping

At this point, the call is connected, and the eavesdropper can hear all sounds from the spied-on phone. Since the speaker of the spied-on phone is disabled, any noise generated by the eavesdropper will not be detected by the victim. In this scenario, the originating switch and the terminating MSC exercise the standard SS7 call setup procedure and do not detect the eavesdropping activity. If the calling party is not the eavesdropper, the call is set up as a normal call. Therefore, the victim can receive calls from other normal calling parties.

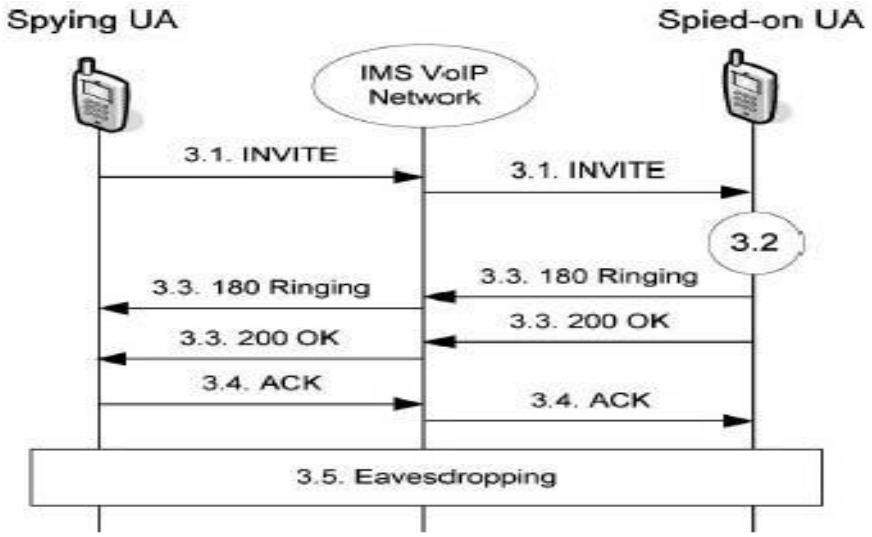

Fig. 6 VoIP call SIP signaling during eavesdropping

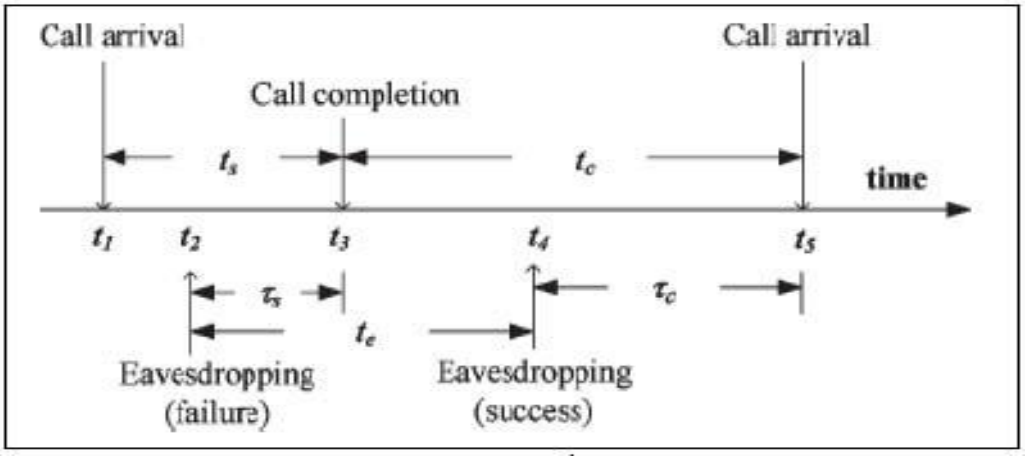

Fig.7 Timing diagram of eavesdropping behavior

When an incoming call arrives during an eavesdropping Session, the eavesdropping session is immediately terminated, and the newly arrived call is connected. Therefore, the victim will not lose any normal calls. The same scenario could be applied on a VoIP network and its signaling description is shown in figure 6. Accordingly, The eavesdropping scenario works as follows.

i) The eavesdropper purchases the spied-on mobile phone. The phone is initially set up with the eavesdropper's phone number as the caller ID that will trigger the eavesdropping procedure shown above.

ii) The eavesdropper gives this mobile phone to the victim (e.g., as a birthday gift).

5.3. Mathematical Modeling of Scenario

The potential eavesdropping period τc = t5 − t4 I n Fig. 7 is the excess life of tc. Since the eavesdropping attempt is a random observer, the expected potential eavesdropping period E[τc] can be expressed as [4]. Suppose that tc has an arbitrary distribution with the mean 1/λ and the variance Vc. Since E[tc] = 1/λ and Vc = E[t2c] − E[tc]2, (3) is rewritten as

$$E[\tau_c] = \frac{1}{2\lambda} + \frac{\lambda V_c}{2} \quad (5)$$

The equation indicates that E[τc] is an increasing function of Vc. As Vc increases, more longer and shorter tc periods are observed. Since the successful eavesdropping attempts more likely fall on longer tc periods, more longer τc periods are observed. Therefore, the expected potential eavesdropping period increases as Vc increases.

5.4. Discussion

So, according to the problem modeling, it became clear we need first to track the potential attacks through real time measurement of tc and τc, then calculation of the Vc. If the value exceeds a certain pre-specified threshold according to algorithm discussed in (3), then there is a possibility of attack. The calls scope could be narrowed down form the statistical view to specific calls according to a convenient database queries getting the corresponding calling-called ID pairs list to form suspecting list. Then, the call behavior of the suspecting list could be tracked further in a close follow up manner to view the performance of those pairs together, the holding time of calls, the response time is the same or different, the ringing duration per caller-called pair. This type of data mining that is based on the reliable database coming from the signaling network is absolutely achievable independent of the OMC, and switching elements, giving the power of correct vision to the network according to the policy, network operators prefer to apply.

6. Case Study: GSM Network Signaling Analysis

As a proof of concept, a real 10 million subscriber network are selected as a practical case study, and some signaling measurements are taken and performance metrics are calculated based on the aforementioned technique to highlight the importance, the information depth, and the reliability that the technique could add as a value to performance improvement and thus cost effectiveness.

The assessment scope of work includes one of the top congested cells of a GSM/UMTS operator, the assessment aspects includes both the radio segment and the network core segment, in addition to the behavioral dimension of the users of the voice service. From this perspective, several pictures are taken from the network based on the A-interface signaling parameters extraction. By definition, a high radio network QOS means that call success rate is high while call establishment and a call release are also successful.

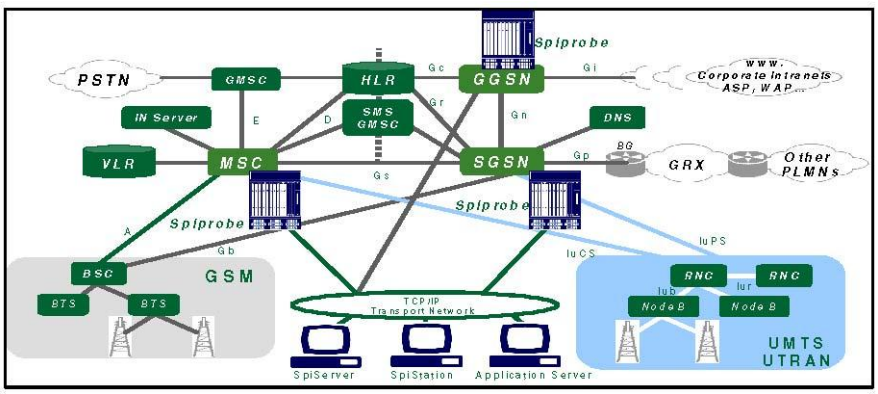

Fig. 8 Typical GSM Network Monitoring Architecture

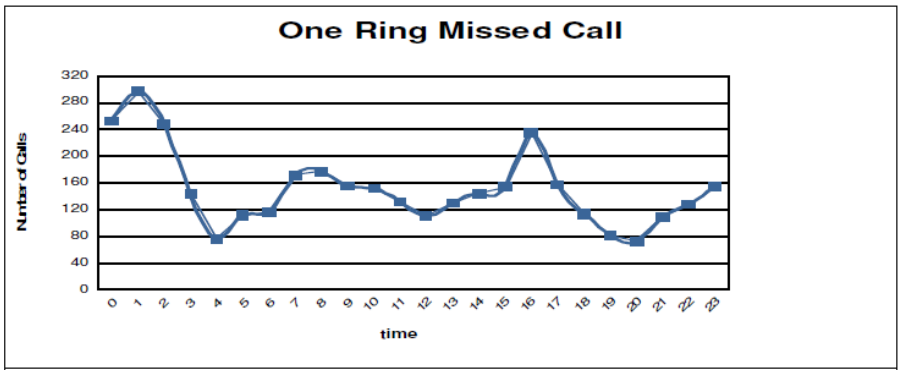

Fig. 9 A Graph showing plot of missed calls resolution using signaling analysis

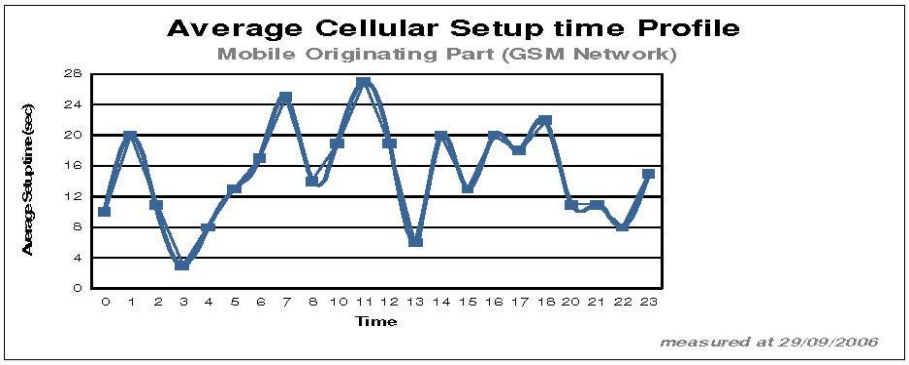

Fig. 10 Average call setup time versus day hours

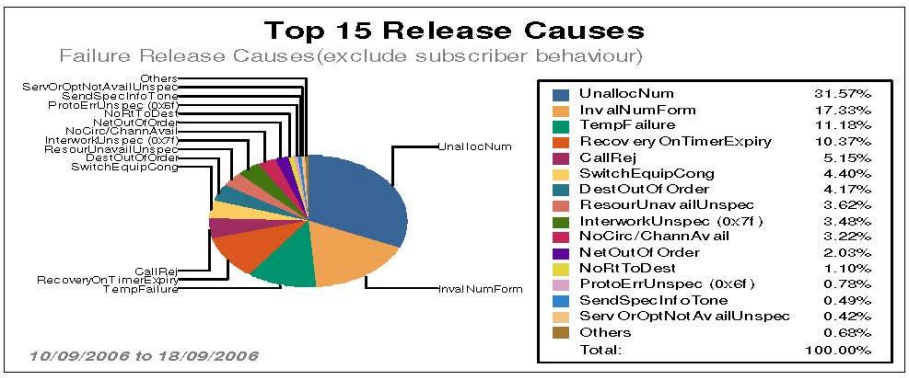

Fig. 11 Handover requests plot versus day hours

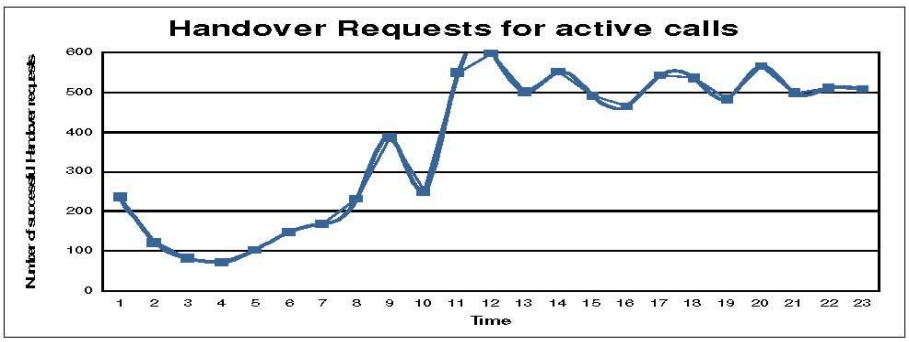

Fig. 12 Call Release Statistical distribution for 8 days capture

The plots in Figs. (9), (10), (11), and (12) show the level of resolution that could be reached. For instance, the one missed call profile is one of the essential profiles required in security cases explained above, as the calls answered after one missed call with a specific statistical distribution are suspicious calls for potential attacks. Also, the other face of the coin, which is the calls that is characterized by ringing without answering, is a phenomenon that is common especially in developing countries, this type of detection helps in determining the network resources utilized due to this behavior, as well as the right level of traffic dimensioning. Based on that, some corrections may be done as priority configurations on some network elements. Similarly, the release root cause analysis, that is useful in excluding the subscriber behavior in the assessment of network performance to give a good indication of the right status of the network as shown in Fig (12).

7. Conclusion

The signaling networks could be used to detect network events including quality levels, abnormal subscriber's behaviors, and network components performance regardless of the manufacturer's proprietary designs, architectures or protocols. The probing of the signaling network could be executed from central focal points that could reflect the majority of performance of the network and decreasing the cost needed to monitor the entire network.

In addition, the mechanism adopted which is passive packet extraction and further post processing techniques gives a lot of flexibility on applying mathematical modeling and analysis separately from the in-service network components relieving the computational load on the network layer. This is explained in the two case studies which are the network security example and the mobile network subscriber behavior example.

As a conclusion, the proposed mechanism helps in simplification, quickness, and accuracy of measurements and analysis regardless of the manufacturer proprietary applications, and nodes architectures.

8. Acknowledgment

A lot of people help us to achieve these results, I would like to express sincere gratitude to Prof. Dr. Abdulhalim Zekri, Ain Shams University for supervising and guidance of this research works. Also, many thanks to Tektronix USA team that support us technically throughout the practical phase, and help us on the physical deployments of test beds and labs. Moreover, my indeed thanks is to Vodafone Egypt that gives the convenient environment for practical analysis.

9. References

[1] Gunnar Heine, GSM Networks: Protocols, Terminology, and Implementation, ISBN 0-89006-471-7, 1999 Artech house, Inc.

[2] William C. Hardy, QoS Measurement and Evaluation Telecommunications Quality of Service, Wiley, 2001.

[3] Breda, G.D., Mendes, L.de S. "QoS monitoring and failure detection" Telecommunications Symposium, 2006 International Issue Date : 3-6 Sept. 2006 ,On page(s): 243 -248 .

[4] Yi-Bing Lin ; Meng-Hsun Tsai, "Eavesdropping Through Mobile Phone " Vehicular Technology, IEEE Transactions , Volume : 56 , Issue:6 On page(s): 3596 -3600

[5] W. Dong; W. Quan-yu; Z. Shou-yi; L. Feng-xia; W. Da-zhen, "A feature extraction method for fraud detection in mobile communication networks", in Intelligent Control and Automation, vol.1, pp: 1853-1856, June 2004.

[6] S. Rosset, U. Murad, E. Neumann, Y. Idan, G. Pinkas, "Discovery of fraud rules for telecommunications-challenges and solutions", in Proc. ACM SIGKDD International Conference on Knowledge discovery and data mining, pp: 409-413, August 1999.
[7] Travis Russell, Signaling System No. 7, Fourth edition, McGraw Hill, ISBN 0-07-138772-2, 2002.
[8] www.ietf.orf/rfc
[9] D.R. Cox, "Renewal Theory", Mthuen & Company.LTD, 1970;
[10] G. Nunes, "Probability Theory and Renewal Theory", Curse of Probability theory applied to Engineering, 2001, unpublished.
[11] W. Feller, "An introduction to Probability Theory and Its Applications – Volume 1", Chapter XIII, p. 303-341, John Wiley & Sons, Inc, 1968.