External, Network-Wide Monitoring of SS7 Networks: A Solution to Managing Digital Telecommunications Networks

Giovanni Marotta, Richard Brown
Networks and Communications Laboratory
HP Laboratories Bristol

HPL-93-63
July, 1993

signaling networks, network management, service integration, traffic forecasting, optimization, mobile communications, intelligent networks

This paper discusses how a switch-independent, network-wide monitoring system for SS7 [1] networks can provide a powerful solution to managing the complex requirements of modern digital telecommunications networks.

The proposed approach to SS7 traffic monitoring allows the provision of a homogeneous view across networks independently of multi-vendor switch hardware and software, thus overcoming the limitations of traditional tools such as network element built-in management and local protocol analysis. It provides the global network view aimed at by SS7 OMAP [1] requirements in a robust and effective way.

The logical architecture of a prototype built-on monitoring system is shown, on which management applications are being developed.

Practical examples of applications in the operational surveillance and investigation areas are also given.

External, network-wide monitoring of SS7 networks: a solution to managing digital telecommunications networks.

Authors: Giovanni Marotta, Richard Brown.

Hewlett-Packard Laboratories, Bristol

Filton Road, Stoke Gifford,

BS12 6QZ Bristol (UK)

Tel: +44 272 228742

Fax: +44 272 228924

Email: gm@hplb.hpl.hp.com

ABSTRACT

This paper discusses how a switch-independent, network-wide monitoring system for SS7 [1] networks can provide a powerful solution to managing the complex requirements of modern digital telecommunications networks.

The proposed approach to SS7 traffic monitoring allows the provision of a homogeneous view across networks independently of multi-vendor switch hardware and software, thus overcoming the limitations of traditional tools such as network element built-in management and local protocol analysis. It provides the global network view aimed at by SS7 OMAP [1] requirements in a robust and effective way.

The logical architecture of a prototype built-on monitoring system is shown, on which management applications are being developed.

Practical examples of applications in the operational surveillance and investigation areas are also given.

KEYWORDS

Signalling Networks, Network Management, Service Integration, Traffic forecasting, Optimization, Mobile communications, Intelligent networks.

1. INTRODUCTION

This section discusses current issues and technical solutions in SS7 network management.

1.1 Current issues

As user needs increase, demands on digital telecommunications networks grow at a dramatic rate. Providing appropriate responses to requirements, such as quality of service, traffic control, network design, new services planning and integration, will constitute the key differentiator for telecommunications operators to be successfully present in the market.

Signalling systems have evolved with the growth and evolution of the telecommunications networks they serve. What once was a simple mechanism managing call setup, call cleardown and billing is now a sophisticated system capable of optimising the operation of the digital telecommunications network and supporting current and future services. As well as providing faster call setup/release and higher reliability, SS7 enables the development and deployment of "intelligent" network services, such as 800 free-phone and GSM [6] mobile telephony both nationally and internationally.

However, SS7 is mainly software based and it has experienced catastrophic failures leading to massive losses in subscriber service, revenue and its claim to reliability. Such losses can run into millions of dollars.

Software problems are particularly difficult to track down in large distributed systems. In many situations, they tend to propagate uncontrollably or trigger off other problems, making troubleshooting operations very difficult and time consuming, and the whole telecommunications networks unavailable for hours [3].

1.2 Current solutions

Traditional methods of managing these crashes, are either based on:

✦ *SS7 network element management*; or

✦ *local protocol analysis*.

SS7 network element management deals with measurements made on the signalling network resources, also known as 'primitive measurements' [1], which are stored within the signalling points. Network element management is also referred to as 'built-in' management.

Primitive measurements encompass signalling links performance, availability and utilization, signalling link sets and route sets status and utilization, ISUP, SCCP, and TCAP utilization and performance [1]. These measurements may be used by test and maintenance procedures (OMAP) to provide both a local view and 'global network view' [1] of the performance of the signalling network.

However, this approach has turned out to be ineffective in most situations for the following reasons:

- ✦ their outputs lack a global understanding of the arising problems in real time. This is because the range of measurements and maintenance procedures is still incomplete and nebulous;
- ✦ a switch's primary function is to switch traffic, not provide statistics. When a network becomes stressed, and information on what is happening is most needed, switches will rarely provide the measurements and the operators have to run "blind".
- ✦ SS7 management data is often available in fifteen minute averages, missing practical timeliness requirements, which are key to proactively managing the telecommunications network.

Local protocol analysis is realised by means of measurement boxes, such as protocol analysers, which provide very detailed information from a few links of the network by decoding the SS7 messages being captured. This diagnostic tool can rarely give an appropriate solution to surveillance problems for the following reasons:

- ✦ protocol analysers are being used in a fire fighting mode, not for proactive management. An operational fault must first be detected and localised prior to taking preventive actions;
- ✦ local protocol analysis misses the target of a high-level view of the problem. This doesn't always guarantee the identification of the source and type of a complex problem.
- ✦ this approach is costly and time consuming. Usually, an SS7 protocol expert has to be dispatched to where the source of the problem has presumably been localised.

Given the inadequacy of these traditional solutions, breaking fresh ground is therefore needed in SS7 management.

2. EXTERNAL, NETWORK-WIDE SOLUTION

The proposal of an ***external*** SS7 monitoring system is a solution to the requirement of a system which must always remain dependable, and continuously provide meaningful information on the health of the network in sufficient time for corrective actions to be taken. The external system consists of distributed instruments fully 'built on' the monitored SS7 network, as shown in section 5.

The ***network-wide view*** is necessary to overcome the limitations of the local approach, which is unable to provide an understanding of the network behaviour. Network-wide means that SS7 data is collected from all over the network, meaningfully correlated and presented in a timely fashion.

The realisation of a network-wide view is facilitated by the provision of an external SS7 monitoring system. Hence, most features of the system proposed in this paper are the outcome of the combination of the two aspects.

A list of the features provided by the external, network-wide SS7 monitoring system is shown below:

- ***robustness.*** An external, built-on monitoring system does not fail when the monitored network fails;
- ***continuous monitoring.*** A dedicated, external monitoring system can provide its data collection and correlation functionality continuously;
- ***timeliness.*** A careful choice of architecture, measurements and applications is essential to provide timely responses to arising problems;
- ***homogeneous view.*** The network-wide view provides a powerful means of characterizing the normal behaviour of a heterogeneous network consisting of network elements from various manifacturers. Hence, being able to detect deviations from the nominal behaviour of the network will represent the key to generating warnings and alarms;
- ***scalability.*** New measurements and applications can be deployed on an external system at considerable speed, without affecting the upgrade of SS7 software throughout the signalling points/ switches, which can be a notoriously long process, especially for multi-vendor software.
- ***strategic view.*** The network-wide view allows and encourages the development of strategic applications in the areas of network and service planning.

The last point highlights the fact that an external, network-wide view of the SS7 network represents the unifying concept for a system capable of both managing proactively a telecommunications network in critical situations and addressing long-term strategic needs of telecommunications network management, such as network characterization, optimization of service provision, and evaluation of teletraffic changes on introduction of new services.

3. TECHNICAL CONSTRAINTS AND SOLUTIONS

This section discusses the technical constraints of a real-time SS7 monitoring system tackling stringent operational surveillance requirements, and presents the associated solutions of the external, network-wide system.

- *Characterization of measurements.*

Prior to placing thresholds and generating warnings and alarms, it is important to characterize the nominal operational state of the SS7 networks. One essential requirement for achieving this is the notion of normalization of measurements and threshold across the different parts of the network. The external, network-wide monitoring system can give an answer to this problem by analysing SS7 traffic trends and load throughout the network for a period of time. The network manager can therefore decide with more confidence what measurements and applications are essential to represent the nominal behaviour, and what normalization factors should be applied for the same thresholds on different sections of the network. Deviations from the assessed nominal behaviour will generate warnings and alarms.

✦ ***Data Reduction.***

A monitoring system for SS7 is required to handle hundreds of 64 Kb/sec channels of SS7 traffic across geographically distributed signalling points. There may be the need to reduce the input rate for two reasons: providing the operator with intelligible information and avoiding overload in the monitoring system itself. One approach is to reduce the SS7 data in a statistically robust way [4], given that most measurements are based on statistical notions. Also, choosing to measure only those measurements reflecting the network behaviour will make the system achieve the timeliness requirements of an 'early warning'.

✦ ***Time synchronization.***

Data correlation is only achievable across the network if the captured SS7 messages are timestamped by the dedicated hardware. Therefore, the use of time synchronisation protocols, such as the Network Time Protocol (NTP) [5] allows the synchronization of remote monitors within 10ms.

✦ ***Provision of measurements.***

Choices of the system design are made in order to have the output data presented at different levels of detail and scope, bearing in mind that they must provide a guided discovery to the source of the problem, from a very high level point of view down to a suitable level of analysis. Functionally, general purpose data correlation procedures provide the monitoring applications with a variety of differentiated pieces of information from the same captured data.

4. SYSTEM ARCHITECTURE

This section briefly presents the logical architecture of the prototype SS7 external, network-wide monitoring system. This architecture is an essential piece of the overall system design able to address and solve the issues discussed in previous sections.

Figure 1 shows how the external SS7 monitoring system (drawn in thicker lines) maps logically onto the digital telecommunications network.

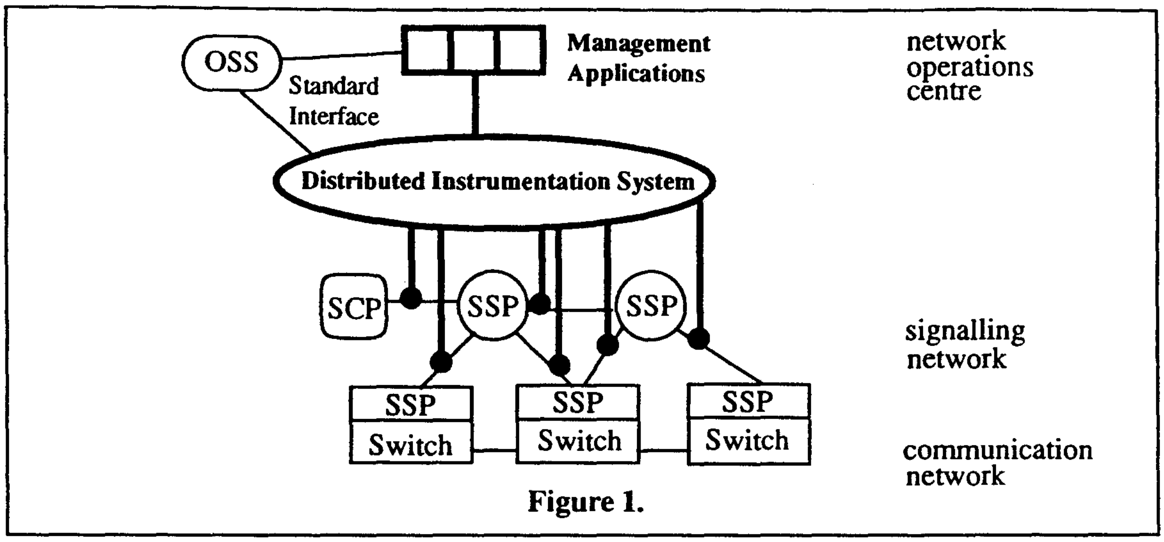

Figure 1.

Figure 2 shows a possible implementation of such an external distributed instrumentation system, with built-on networked equipment.

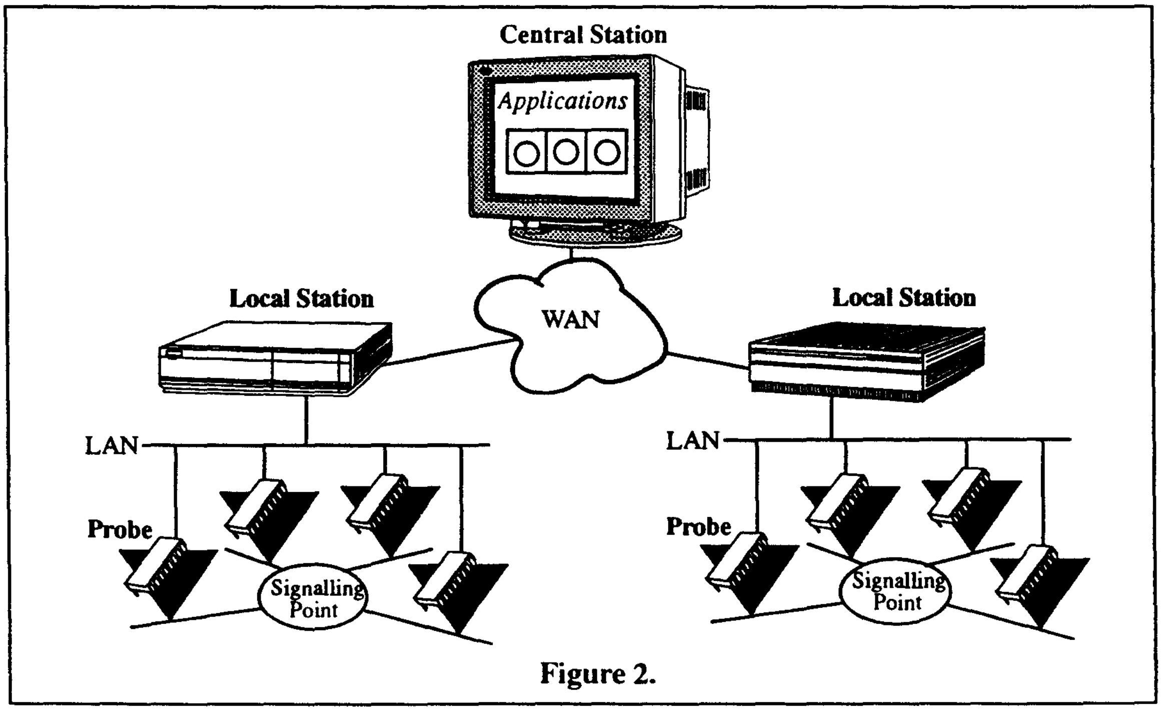

Figure 2.

It consists of dedicated low-cost hardware probes connected to the SS7 links which continuously capture SS7 traffic; processing agents distributed across different hardware and locations for data reduction, storing and correlation; a communications infrastructure between monitored points and monitoring centres; and, the network management applications. The probes represent the dedicated SS7 interface hardware, the local sites are the locations where data storing and correlation are performed, and the central site is where the network-wide management applications run.

Let's now show how such a system can be used in several areas of SS7 monitoring.

5. THE NETWORK-WIDE VIEW IN OPERATIONAL SURVEILLANCE

Failures in SS7 operations have led to catastrophic crashes of the SS7 networks, making the whole telecommunications networks unavailable for hours [3]. The cost of such failure has been high. Real-time operational surveillance of the SS7 network is extremely important if early warnings of mounting problems can be provided to allow appropriate controls to prevent telecommunications networks from crashing.

5.1 An application: Traffic Monitor

This section describes the *Traffic Monitor* application, a practical example of Operation Surveillance for an SS7 network, which was developed as part of the prototype SS7 monitoring system.

Figure 3 shows the top level view of the Traffic Monitor, and considers three different aspects of the behaviour of an SS7 network:

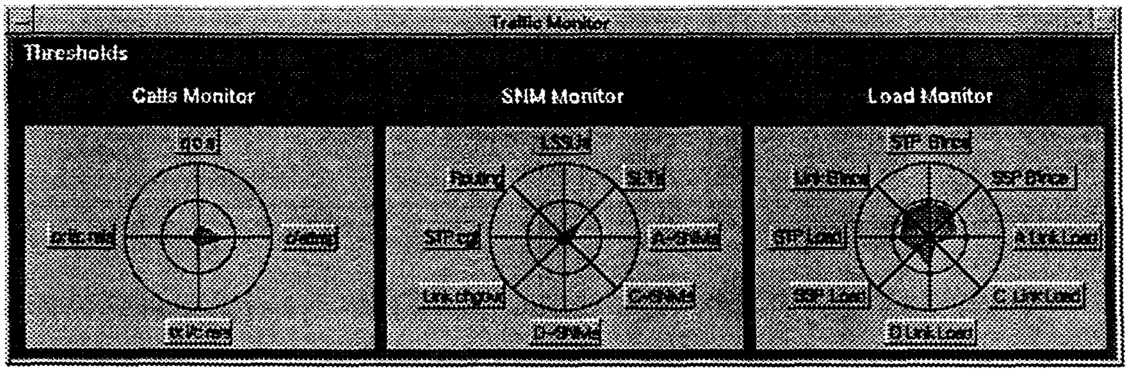

Figure 3.

- ***traffic related to call setup and release (Calls Monitor).*** This characterises the user perception of the quality of service with respect to the voice and data traffic, by monitoring call setup/release ratios and the sources and sinks of abnormal call releases. The same measurement can also be useful in detecting unexpected mass calling events;
- ***SS7 management and maintenance traffic (SNM Monitor).*** This is an indicator of the

actual health of the SS7 network. Growth or total absence of this traffic reveals that some problem is building up in the network;

✦ ***absolute and relative load (Load Monitor).*** Unacceptable increase in link load and signalling point load are often leading indicators of potential network failures. However, because traditional built-in management often fails under such circumstances, measurements provided by the load monitor become the only source of information about the network state. Even if the network performs "normally" from the user point of view, it may well be that load imbalances across links and signalling points in the background will cause the SS7 network performance to drop quickly during emergency situations.

The Traffic Monitor consists of three charts, called "radar charts", one for each aspect mentioned above. Each chart has several axes representing normalised measurements and two threshold levels for each measurement, used for generating warnings of deviations from nominal behaviour. When all values are below the inner threshold the chart is green and the network state is regarded as normal. If at least one measurement crosses the inner threshold then the chart will go yellow, meaning that somewhere in the network a problem may be developing. If a measurement exceeds the outer threshold then the chart will go red, that is a problem is present and immediate action is required.

It is worth noticing that this top level view displays the worst/most significant case of each measurement across the network. Clicking on an axis provides a first level breakdown of the selected measurement, typically the top ten SS7 network elements contributing to that measurement or being affected by the abnormal situation. Selections on the nested diagrams will provide further breakdowns that will guide the operator to the discovery of the source and nature of the problem.

5.2 Congested STP scenario

The following example is part of the literature of SS7 failures. It is a complex scenario where a minor fault triggers off a major one causing the SS7 network to crash. In the example, we give a brief explanation of the minor fault, and show how the Load Monitor reacts as the major fault develops. We could have equally shown how the SNM Monitor would have been able to detect the triggering event, thus providing the operator with the opportunity to take early actions and prevent the major problem from occurring.

Figure 4 shows the SS7 topology where our example takes place.

The topology includes a collection of Signalling Service Points (SSP) or end offices and a mated Sig-

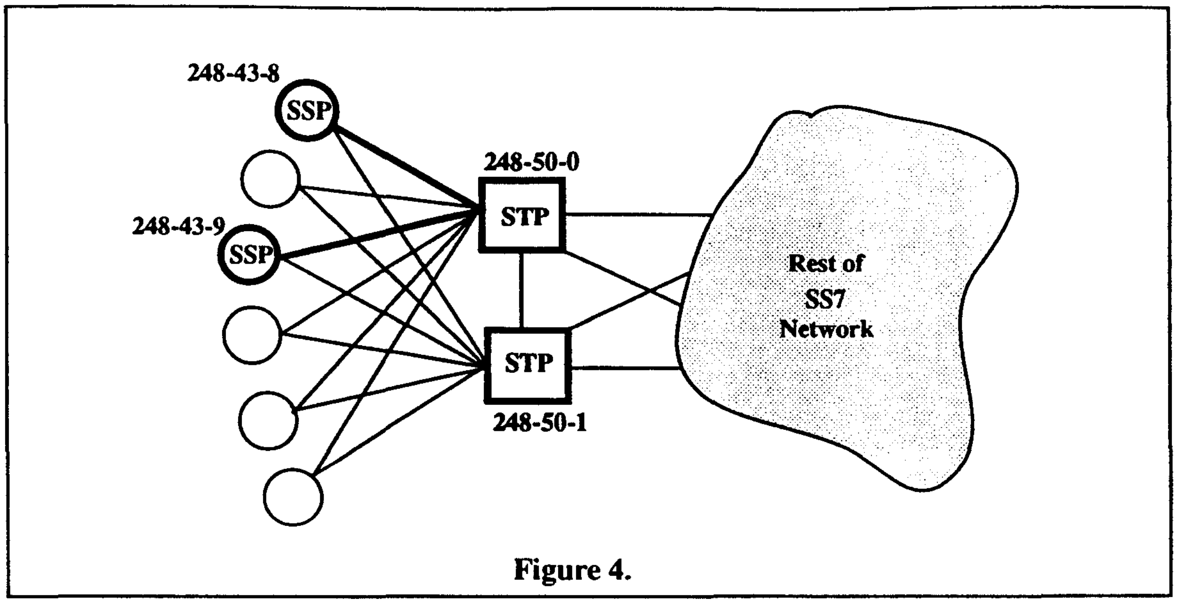

Figure 4.

nalling Transfer Points (STP) pair. The failure scenario begins with a hardware problem causing the links between STP 248-50-0 and SSPs 248-43-8, 248-43-9 to go in and out of service repeatedly: bouncing links. This behaviour creates extra load at the STP internal Tx/Rx buffers. Unfortunately a well known software bug causes the internal congestion control mechanism to get switched off at the STP, so that it cannot tell the rest of the network that it is becoming congested. Eventually, the STP overloads and SS7 traffic can no longer be transferred through it.

Let's see how the Traffic Monitor reacts to this final situation. Figure 5 shows that the Load Monitor chart on the right-hand side presents some measurements having crossed the outer threshold.

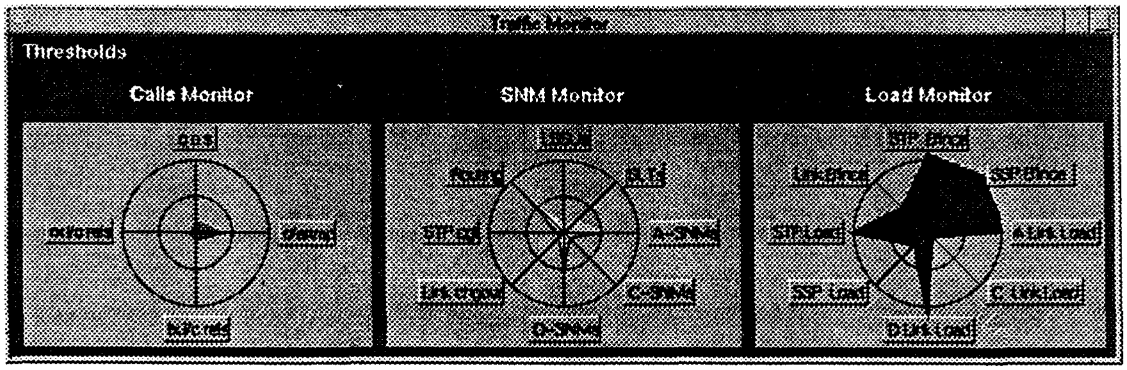

Figure 5.

Clicking on SSP balance will make a "top point codes" diagram to pop out (figure 6).

It can be noticed that all SSPs shown are experiencing the same imbalance with respect to the load sharing between the STP mated pair.

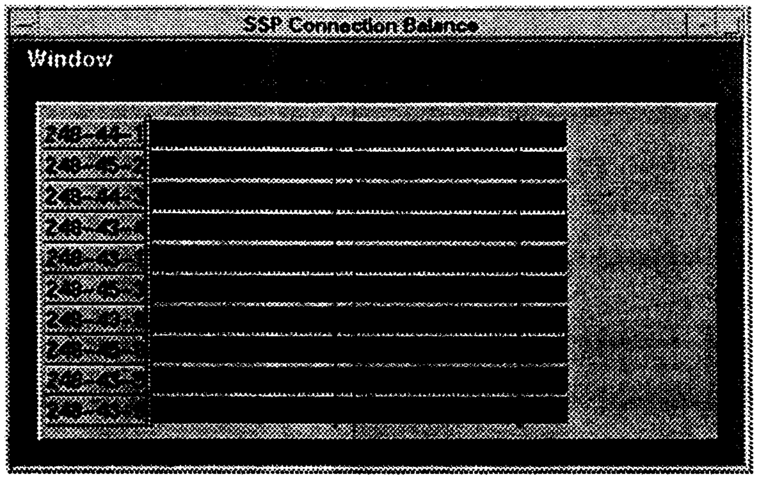

Figure 6.

It is possible to view a further breakdown by selecting one of the SSPs. The result of this (figure 7) shows that over the last four minutes the connectivity between STP 248-50-0 and SSP 248-44-1 has been lost, thus confirming the first level analysis.

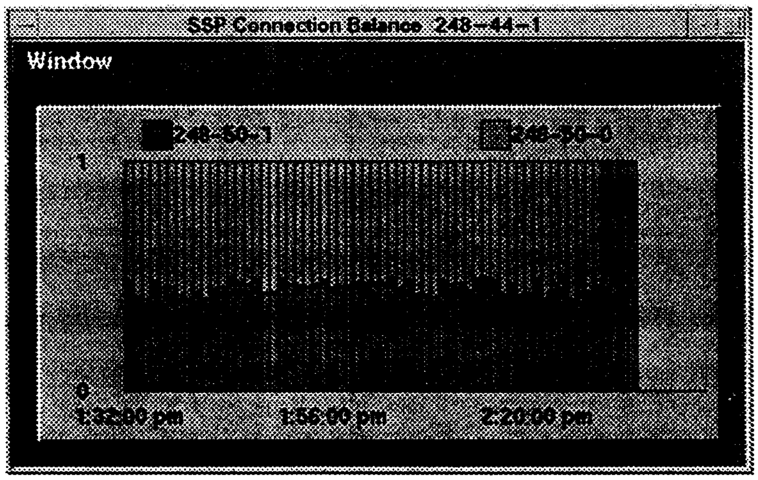

Figure 7.

At this point the operator should take proper action before the problem propagates all over the network. The effects of isolating the oscillating links and the faulty STP plus reducing the SS7 traffic rate at the SSPs can be validated in real time with the Traffic Monitor.

6. THE NETWORK-WIDE VIEW IN INVESTIGATION AND DIAGNOSIS

In some cases a specific analysis of "what is going on" is necessary when a problem is not addressable by using statistical measurements. This area is identifiable as 'investigation and diagnosis' and, historically, it has been the first one to be tackled by early instrumentation for SS7 networks.

These instruments, namely protocol analysers, provide very detailed information from a few links of the network by decoding the SS7 messages being captured, but they are not particularly effective for proactive management of the network.

5.1 Distributed Protocol Analysis: an example

By using external hardware to fully monitor the SS7 network, the traditional local protocol analysis now becomes distributed protocol analysis, and it can be readily integrated in the external SS7 monitoring system design as a component of a set of "on demand" tools. The notion is that some applications are not permanently active, but they are deployed when an external event makes this necessary. On deploying an "on demand" application, the dedicated SS7 hardware and the processing agents covering the section of the network under investigation will capture and correlate all the SS7 traffic concerning a particular service from a specific area. This is not at the cost of the operational surveillance measurements and applications, which will continuously run in the background.

An example of such an 'on demand' tool is when an alarm, generated by the operational surveillance, requires very focused analysis on specific SS7 traffic over a certain geographic area. Similarly, a customer complaint about the provision of a network service may require investigation.

Consider the following situation: a customer claims that calls to its 800 number are not being distributed correctly across the various sites of the company. To verify this, the network operator decides to deploy distributed protocol analysis on all the links surrounding the Signalling Control Point (SCP) providing the translation for that 800 number (figure 8) from the network management centre.

Particular software filters are applied in order to capture, decode and correlate only SS7 SCCP response messages related to 800 services, carrying the real telephone numbers belonging to the customer. On the operator central console, a real-time graph provides a statistical view of the calls being distributed among the sites, so as to assess whether the customer complaint is supported by facts.

The advantages of this distributed approach compared to the traditional local protocol analysis are numerous:

- ✦ the operator can deploy the distributed investigation from a central console and get the output on the same device, without dispatching engineers all over the place. An imperfect understanding of the placement of the measurements can therefore be easily corrected at virtually no extra cost;

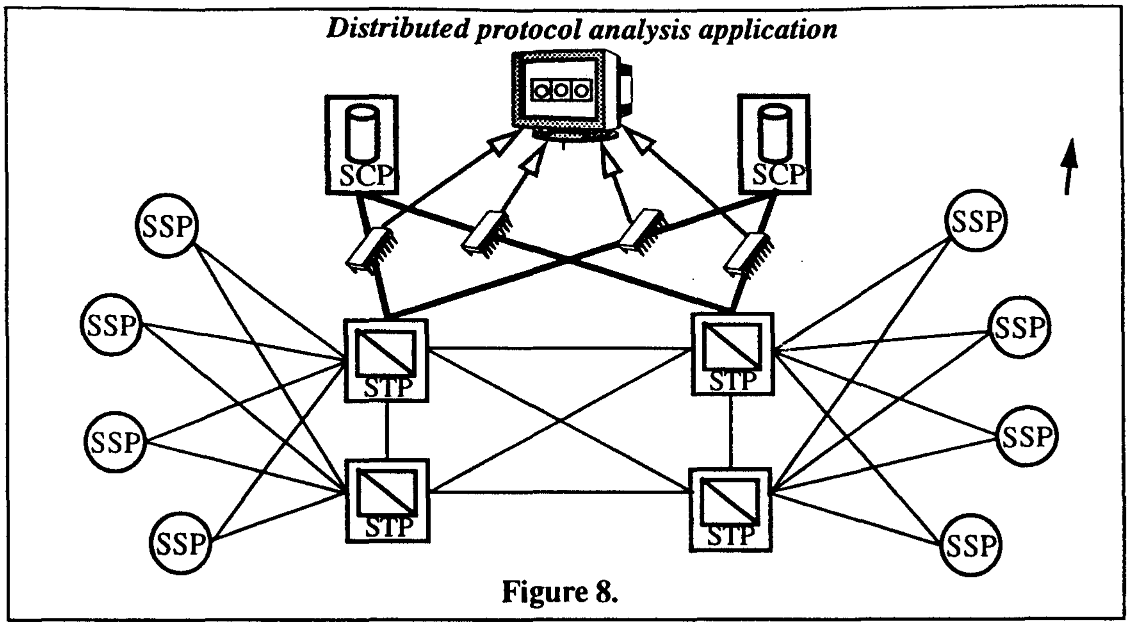

Figure 8.

- ✦ activating software filters carefully allows the data correlation processes to work on a essential collection of data;
- ✦ the output of an investigation is presented in a understandable fashion, not just as a collection of unrelated protocol analysis screen dumps. Hence, the problem can be understood and solved in a timely fashion.

7. THE NETWORK-WIDE VIEW IN THE STRATEGIC DOMAIN

This section discusses the longer term demands that a telecommunications network must satisfy in the strategic management of the network. Most strategic applications of the external SS7 monitoring system rely on the provision and analysis of a history of the state of the SS7 network. These applications are collectively referred as "historical applications" in the rest of the paper.

7.1 Network management

As previously stated, most network operators struggle to identify the nominal behaviour of their networks. This weakness will consequently affect the identification process of deviations from the norm, which is key to placing thresholds and generating warnings/alarms.

An historical application, which analyses the SS7 traffic trends and load throughout the network for a long period of time, can help the network manager decide with more confidence what thresholds to place across the network.

In the longer term, historical applications can support the operator in identifying traffic peaks, steady modifications of the average traffic, and unexpected patterns at some locations or in certain hours. In other words, they can support all the tasks of a traditional network management centre.

Historical applications can also be used to help the network planner model a network. For example, if we decide to add a new signalling code, the consequences of this introduction can be checked against the external system with respect to traffic load distribution, quality of service, and so on.

7.2 Services management

Apart from controlling the usual voice/data traffic, SS7 was also introduced to satisfy the demands of business and domestic subscribers for new, sophisticated services (e.g. 800 numbers).

The SS7 protocol stack contains a part for providing transaction-oriented capabilities (TCAP) [1], a mixture of OSI-like transport and application layers [2], which the provision of these sophisticated services relies on.

One main management goal is therefore to ensure that the quality of these advanced services meets the expectations set for the customers.

When it comes to checking that the deployed service is behaving correctly, a distributed, customised protocol analysis application of the external system would be of great value. One should not forget that optimum deployment of services would improve their quality and would prevent the signalling network from being overloaded with avoidable SS7 traffic.

A network-wide historical analysis of traffic trends for a service under investigation would give clear indications on how a service provider should be moved or duplicated in order to limit the SS7 transaction messages to that service provider within a smaller and more easily manageable SS7 island. A similar analysis would also help the service planner make cost/benefit judgements about the long term evolution of the network services.

It is clear that the introduction of new services on test or live networks would also be positively supported by both real-time and historical applications. This becomes increasingly true as the growing number of deployed intelligent services raises the SS7 traffic level.

8. FUTURE APPLICATIONS: MOBILE COMMUNICATIONS

The dramatic growth of mobile radio systems will affect the SS7 traffic profile of the telecommunications networks, since the signalling demands of these systems are orders of magnitude greater than for the fixed network.

In Europe, the mobile system GSM [6] is meant to transmit its land-based signalling messages over SS7, so that both fixed and mobile network operators will have to cope with unusual levels of SS7 traffic.

A few reasons for this increase are:

- ✦ inherent complexity of the signalling part of the GSM standard reflecting the variety of intelligent functions required to achieve the goals of mobile systems;
- ✦ increased length of SS7 messages;
- ✦ growth of failed call attempts, due to the poorer end-to-end quality of service of mobile calls.

It is even clearer that in the case of mobile communications the network-wide approach for monitoring SS7 signalling is crucial. In this scenario, the notion of user mobility implies a monitoring system based on statistical analysis, both for real-time operation surveillance and historical traffic trends.

Furthermore, since the signalling for GSM is mainly "intelligent", what has been said about service monitoring, optimization and placement will find fertile ground in the mobile world, thus causing an effective network and service management system to be indispensable.

A real example is the provision of the Short Message Service (SMS). This service allows short text messages to be sent and received over the signalling network by suitable equipped GSM handsets.Theoretical analysis [7] have shown that for high take-up of the service the impact on the SS7 signalling can be significant. Furthermore, the network resources would have to be carefully planned and monitored depending on the expected take-up rate.

9. CONCLUSION

This paper has shown that a monitoring system for SS7 networks, which is realised with built-on instrumentation fully covering the SS7 elements, is capable of providing the global network view as encouraged by SS7 OMAP requirements in a robust and effective way.

Appropriate choice of measurements and technical solutions are key to providing powerful applications handling several aspects of the SS7 management, such as operation surveillance, investigation and diagnosis, network and service management.

Since the SS7 is the central nervous system of the modern digital telecommunications system,

the belief is that such an external monitoring system can provide a more global solution for the needs of today and the demands of tomorrow to the telecommunications operators.

ACKNOWLEDGEMENTS

This paper would not have been possible without essential contributions from the following people: Olivier Beneteau, Steven Bennett, David Clarke, Mark Easton, Toby Ferguson and Peter Mottishaw.

REFERENCES

[1] "Specifications of Signalling System No.7", CCITT Blue Book - Recommendations Q.700 to Q.795, Geneva 1989.

[2] U. Black, "Network Management Standard", McGraw-Hill, Inc., 1992.

[3] "Preliminary Report on Network Outages", FCC Common Carrier Bureau, July 1991.

[4] J. Jedwab, P. Phaal, B. Pinna, "Traffic Estimation for the Largest Sources on a Network, Using Packet Sampling with Limited Storage", Hewlett Packard Labs, Bristol, Technical Report, HPL-92-35, March 1992.

[5] D.L. Mills, "Measured Performance of the Network Time Protocol in the Internet System", ACM Computer Communications Review 20, January 1990.

[6] ETSI/TC GSM Recommendations Series.

[7] M. Beech, B. Bertolino, D. Chan, "Traffic Analysis of the GSM Signalling Network using Model-based Techniques", Hewlett Packard Labs, Bristol, Paper submitted to IEEE JSAC.