Distributed Self Fault-Diagnosis for SIP Multimedia Applications

Kai X. Miao[1], Henning Schulzrinne[2], Vishal Kumar Singh[2], Qianni Deng[3]

[1] Intel Corporation, 2200 Mission College Boulevard,
Santa Clara, CA 95052-8119, USA
kai.miao@intel.com

[2] 450 Computer Science Building, Department. of Computer Science, Columbia University
New York, NY 10027, USA
{hgs, vs2140}@cs.columbia.edu

[3] 1954 HuaShan Road, Department. of Computer Science, Shanghai Jiaotong University
Shanghai 200030 P.R. China
deng-qn@cs.sjtu.edu.cn

Abstract. IP real-time multimedia applications present a challenging environment for network and service management, which requires a new approach. DYSWIS (Do You See What I See), proposed in this paper, is peer-to-peer distributed management architecture for multimedia network and service management, characteristic of active fault probing and identification based on protocol and functional scripting and rules.

Key Words: fault, SIP, VoIP, Internet, IP, quality, QoS, diagnosis, SNMP, P2P

1 Introduction

In spite of the recent growth in Internet multimedia communications, service availability and voice quality of IP-based multimedia applications still falls behind when compared to traditional PSTN voice services, as shown in a recent study [1]. In contrast to PSTN, the Internet decentralizes network intelligence and allows end user devices and local networks to grow significantly in capability and complexity. Yet, the world is still dominated by a centralized service and management model, as in PSTN. In this model, we assume all network elements can be professionally (centrally) managed, a service provider is able to "see" and control every network element, including a user device, and all failures are hard failures thus easily detectable. All these assumptions are obviously no longer true for IT multimedia services and the centralized control model of the past is no longer able to effectively handle the complexity of today's IP network for multimedia services, as is evidenced by failed efforts to solve the service quality problem of VoIP.

In particular, existing network management approaches are limited in cases like residential users for whom there is no IT admin, communications in a rural community where only extremely limited IT support is available, and corporate users having certain transient problems such as telecommuters using networks not owned by their

employer. Traditional problems management is based on a model of "ownership" – by either an IT department or a service provider. In IP multimedia service environment, however, there are many useful service scenarios where a service or device can not be fully owned by a provider or IT. Automatic problem management, including self fault diagnosis and automatic problem fixing capabilities, is crucial and so is a standard based fault diagnosis mechanism so that problems can always be found no matter where they occur. Such a standard is apparently beyond SNMP's capability.

Even for a multimedia service clearly owned by a provider or IT department, managing user devices can be very hard in a world where convergence and divergence of networks and user devices appear to be happening at the same, which makes managing a multi-media service or a user device is a huge challenge. Traditional network management cannot reach into certain user devices and thus cannot easily exclude certain failure causes, in consideration of the fact that many user devices such a PC or SIP phone today are not managed

In the complex world of IP multimedia services, faults can be very elusive, even for experienced IT experts. The same visible problem to a user or an IT admin can be caused by many different root causes, for example, from DHCP address allocation failures (apparently common in large-scale wireless networks) to NAT time-outs and various ISP failures. Harder-to-diagnose "dynamic" network elements such as NATs with binding time-outs or limited binding tables make the traditional management approaches quite ineffective for fault identification.

Following the above discussion, we propose a new and generic distributed network management framework that leverages distributed resources in a network. We call the basic approach "*Do You See What I See*" (**DYSWIS**) [2]. DYSWIS treats each node as a potential source of network management information, gathering data about network functionality and component function availability, performance, and failures. Each participating (DYSWYS) node has a certain capability level for fault diagnosis, from basic failure detection and maintenance of failure history records to the ability to invoke a set of standardized or customized network probing tools within the system (e.g., ranging from versions of "ping" and "traceroute" to more application-specific probing tools) for specific network and application layer protocols and the abilities to learn and track network fault behavior, intelligently create and manage diagnostic tests and perform inference modeling and analysis of faults. Other nodes can ask DYSWIS nodes to report on its view of certain network nodes and services.

In the next section, we will provide more details about DYSWIS.

2 DYSWIS Architecture and Components

Figure 1 shows the fault-diagnosis framework we are proposing consisting of a number of regular nodes and DYSWIS nodes in a network. A DYSWIS node is capable of

local fault detection, communicating fault information with other nodes about network faults, and storing network fault history information.

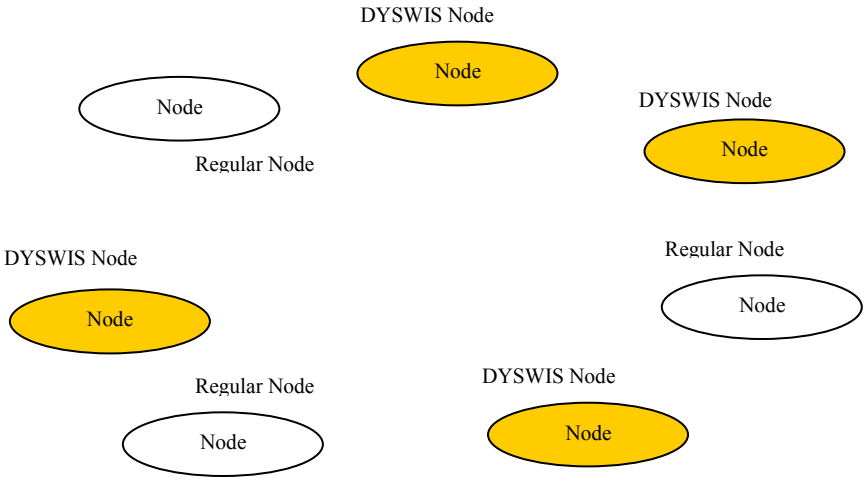

Fig. 1. *DYSWIS – "Do You See What I See"* – Fault Diagnostic Framework

A DYSWIS node is capable of actively testing or probing functions for the purpose of fault identification in a network, which may include gathering properties associated with a multimedia call or collecting historical information. For example, if SIP call set up fails, a node would go through a set of steps, such as sending a ping to the proxy, trying a SIP test server or reaching other nodes on other protocols, to see if the problem is with server reachability, a firewall that blocks SIP messages or general network reachability problems.

DYSWIS nodes are distributed over the network where a multimedia call is made, because, often, the only way to detect a fault is to run tests from multiple vantage points in the network. A problem as experienced by a user can be "far away" from the fault that causes the problem. A local DYSWIS node can work with a remote DYSWIS node to more effectively identify where the fault resides.

DYSWIS architecture can operate in both centralized (client/server) mode and p2p mode. It needs a mechanism for a manager to gather data collected by measurement points in a network, but also needs to function in peer mode when there is no central manager. In p2p mode, each node could monitor its local communications and then trigger a query to peers, following a set script and set of rules, depending on the observed condition.

An extensible set of building blocks in DYSWIS nodes can test protocol functionalities not only along the "path" of a call but also across the network stack, as faults can occur anywhere in the network stack. In addition, a functionality fault needs to be

measured and characterized by different performance levels, in addition to hard failures.

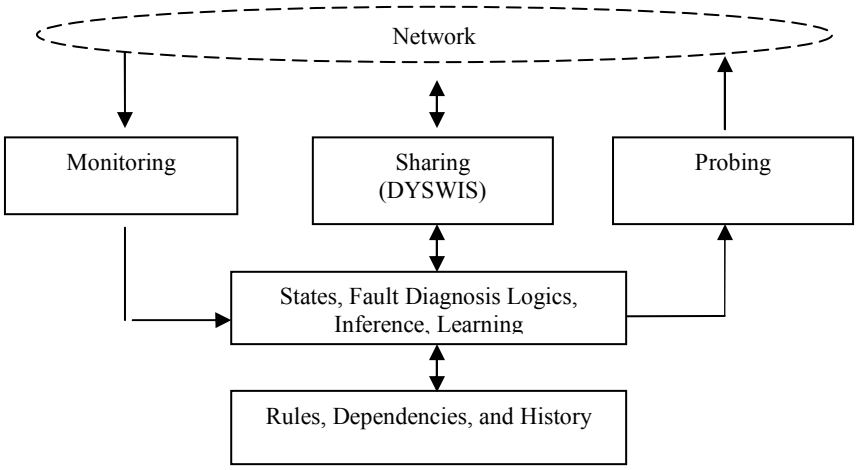

Fig. 2. Functional Components in DYSWIS Fault Diagnosis Framework

Within a DYSWIS node, as shown in Figure 2, the fault management system can be seen as consisting of several key components: monitoring, probing, sharing via a communication mechanism to exchange results (i.e., DYSWIS protocol), a rule-based language or engine that invokes monitoring or probing or sharing, and a database that contains history data, dependencies and rules associated with multimedia calls, etc.

3 Work in Progress

Research is being currently carried out at Columbia University and Shanghai Jiaotong University, following the proposed DYSWIS architecture: 1) Extensive analysis has been done on dependency relationships in SIP multimedia call flows (protocol) and scenarios (functional). Fault detection algorithms have been developed on a real system built with SIP server and client components. 2) Packet sniffing software tools for inspecting multimedia application packets have been developed for media fault detections and analysis. 3) Analysis on fault probing operations based on call conditions described in a scripting language is also underway. 4) Investigation is also underway on how to apply the proposed approach to p2p and s/c models for fault diagnosis in general..

References

1. Keynote VoIP Competitive Intelligence Study, Keynote Systems,, TMCnet July 11th 2005 http://www.tmcnet.com/usubmit/2005/jul/1161904.htm
2. Henning Sculzriinne, Managing (VoIP) Applications, Columbia University, July 2005 http://www.cs.columbia.edu/~hgs/papers/2005/IRTF-management.ppt