로그 분석을 통한 서비스 관리 시스템 설계 및 구현

윤인숙, 장범환, 정태명
성균관 대학교 전기 전자 및 컴퓨터 공학부
e-mail : {isyun,bhchang}@rtlab.skku.ac.kr, tmchung@ece.skku.ac.kr

Design and Implementation for Service Management System Using a Log Analysis

In-Suk Youn, Beom-Hwan Chang , Tai-Myoung Chung
Real-Time Systems Laboratory, School of Electrical and Computer Engineering,
Sungkyunkwan University

요 약

사용자의 요구 사항이 점점 복잡해지고 다양해짐에 따라 서비스의 품질을 향상시키고 개인화된 정보 제공을 위한 서비스 관리 개념이 등장하고 있다. 본 논문은 로그 데이터와 트래픽 정보의 분석을 통한 서비스 관리 시스템의 모델을 제안하고 구현을 통해 주요 기능 및 특성을 알아 본다.

1. 서론

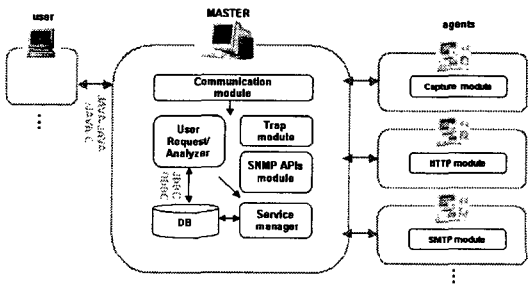
인터넷 사용자 층의 저변확대로 인해 인터넷 접속자 수가 크게 증가하고 있으며 이에 따른 데이터 양도 폭발적으로 증가하고 있다. 인터넷을 통해 교류 되는 수 많은 데이터 중 효과적인 정보 활용에 많은 관심이 모아지고 있으며, 로그 데이터는 관리 대상이 되는 서버에 대한 모든 클라이언트의 접근 및 사용 내역 등에 대한 정보를 기록하여 정보의 질을 높이는 중요한 요소로 자리 매김 하고 있다.

서버는 기본적으로 서버에서 일어나는 모든 사항들을 파일 형태로 남기는 기능을 가지고 있다. 이때 저장되는 파일을 로그 데이터라고 하며, 이러한 데이터는 특별한 형태의 기준에 따라 숫자와 기호 등으로 기록되는데 이 기록은 장비의 종류와 서버 관리자의 선택에 따라 데이터의 형식과 내용이 차이가 날 수 있다. 로그 데이터의 분석을 통해 사용자가 만족하는 시스템을 제공해야 하며 이와 관련해 정보의 통제나 서비스의 적절한 운용을 지원하기 위한 서비스 관리 시스템의 개념이 등장하게 되었다.

본 논문은 분산 환경을 지원하고 플랫폼에 독립적인 JAVA 기술을 기반으로 사용자의 작업을 대행해 주는 에이전트 시스템을 제안하고 HTTP, SMTP 로그 데이터와 트래픽 분석을 통한 서비스 관리 시스템의 모델을 제시한다. 마지막으로 구현을 통해 제안하는 시스템의 기능과 특성을 기술하고 향후 연구 방향을 고찰해보기로 한다.

2. 서비스 관리 시스템 구성

제안하는 서비스 관리 시스템의 구성은 (그림 1)과 같다.



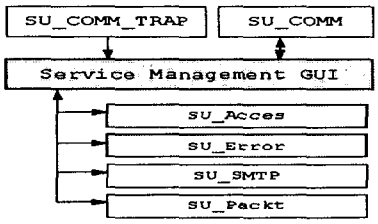
(그림 1) 서비스 관리 시스템 구조

(그림 1)에서 나타나듯이 자바 기반의 서비스 관리 시스템은 사용자의 요구 사항이 시스템에 반영되기 위한 사용자 인터페이스(GUI), 시스템의 모든 구성요소에 대한 관리 책임을 지는 마스터(Master)와 로그 데이터 및 트래픽을 분석하는 에이전트 시스템들로 구성된다. 에이전트 시스템은 SMTP 로그 데이터 분석 모듈, HTTP 로그 데이터 분석 모듈, 트래픽 분석 모듈로 독립적으로 구성되어 있으며 필요에 따라 2 개 이상의 모듈이 에이전트 시스템에 존재 할 수 있도록 구성한다.

3. 서비스 관리 시스템 설계

3.1 사용자 인터페이스

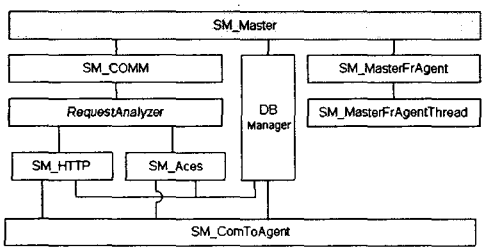
사용자 인터페이스는 사용자가 원하는 작업 요청 시 마스터와의 통신을 담당하는 SU_COMM 모듈, 에이전트 시스템의 예외 사항 메시지를 수신하기 위한 SU_COMM_TRAP 모듈, HTTP 서비스를 제공하기위한 SU_Access, SU_Error 모듈, SMTP 서비스를 제공하기 SU_SMTP 모듈, 네트워크 트래픽을 감시하는 SU_Packt 모듈로 구성되어 있으며 설계 구조는 (그림 2)와 같다.



(그림 2) 사용자 인터페이스

3.2 마스터

마스터는 정보 분석을 대행하는 에이전트 시스템으로부터 로그 파일과 트래픽 정보를 공급 받아 사용자 인터페이스를 통해 서비스를 제공한다. 마스터의 주요 모듈 구조는 사용자가 요청한 작업을 송/수신하는 SU_COMM 통신 모듈, 사용자의 요구를 분석 하여 처리하는 processing 모듈, 에이전트와 SNMP 메시지로 통신하기 위한 SU_ComToAgent 통신 모듈 및 trap 모듈, 데이터베이스를 구성하고 이를 응용하기 위한 DB Manager 모듈로 나눌 수 있으며 마스터의 세부 설계 모듈은 (그림 3)와 같다.



(그림 3) 마스터 모듈 구조.

① SM_Master 모듈

통신을 담당하는 SM_COMM 모듈로부터 사용자와의 연결 설정을 대기한다. 사용자(GUI)의 요청이 있을 경우 연결을 맺은 후 요청 메시지에 따라 분석 처리를 수행 한다. 수행 후 결과를 사용자에게 보내는 역할을 하는 모듈이다.

② RequestAnalyer 모듈

사용자에게 전달 받은 요청을 분석하여 관련 처리 모듈을 호출하고 처리 결과값을 반환하는 모듈이다.

③ SM_HTTP, SM_Aces 모듈

HTTP 관련 서비스 처리를 위한 SM_HTTP 모듈과 SMTP 관련 서비스 처리를 위한 SM_Aces 모듈로써 해당 에이전트와 연계하여 사용자가 원하는 서비스를 제공한다.

④ SM_MasterFrAgent 모듈

에이전트 시스템의 프로세싱 동안에 예외가 발생 했을 때 SNMP 의 trap 메시지를 처리하는 모듈이다.

⑤ SM_ComToAgent 모듈

사용자의 서비스 요청이 에이전트 시스템의 정보를 필요로 하거나, 마스터가 에이전트 시스템에게 관리 정보에 관한 요청이 있을 경우 마스터와 에이전트간의 통신을 담당하는 모듈이다.

3.3 HTTP 에이전트

HTTP 서비스 제공을 위해 관리 대상이 되는 웹 서버에서 동작하는 에이전트로 트래픽 정보, access 로그 파일, error 로그파일 등의 다양한 정보를 수집 분석하는 역할을 한다. HTTP 에이전트의 주요 설계 모듈은 (그림 4)와 같다.

① SA_Agent 모듈

HTTP 에이전트 구성요소의 가용성, 작동 및 관리에 대한 책임을 지는 주요 모듈이다. 통신을 담당하는 SA_COMM 모듈로부터 마스터와의 연결 설정을 맺고 네트워크가 연결되었을 때 HTTP 서비스 관련 스트림을 생성하여 해당 처리 모듈을 수행하는 역할을 한다.

② RequestAnalyzer 모듈

마스터로 요청 받은 메시지를 분석하여 해당 처리 모듈을 호출하는 모듈이다. 웹 서버의 access 로그 파일을 parcing 하는 AccLogAnalyer 모듈과 error 로그 파일을 parcing 하는 ErrLogAnalyer 모듈이 처리한 결과 값을 반환하는 모듈이다.

③ LogFileManager 모듈

Apache 와 IIS 와 같은 이기종의 웹 서버에서 획득한 access 로그 데이터와 error 로그 데이터의 관리를 위해 관리자가 설정한 데이터 포맷에 따라 로그 데이터를 파일 형태로 관리하는 모듈이다.

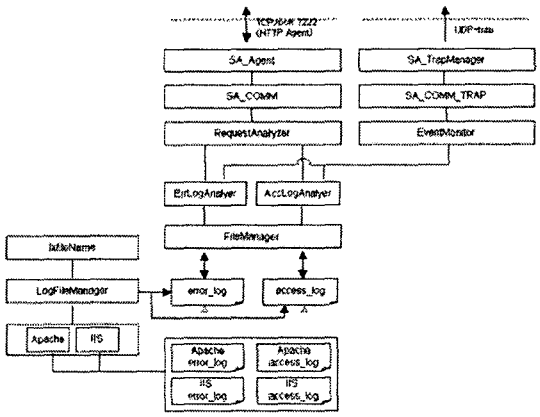
④ FileManager 모듈

LogFileManager 모듈을 통해 로그 데이터의 그룹 관리가 이루어진 후 24 시간 단위로 로그 파일을 백업하여 분석 모듈에게 제공함으로써 에이전

트와 마스터간의 정보 전송의 부하를 줄일 수 있게 한다.

⑤ SA_TrapManager 모듈

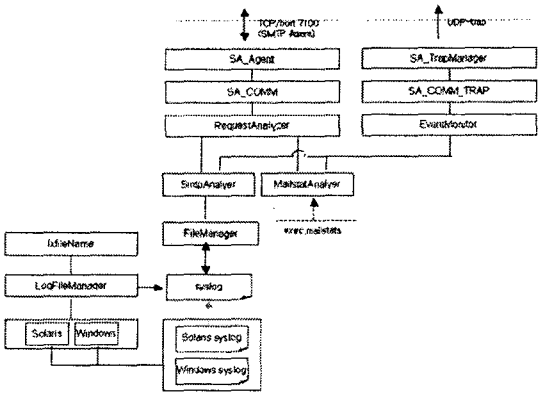
에이전트 시스템이 위치한 웹 서버의 로그 데이터 분석 동안 예외가 발생했을 때 EventMonitor 모듈이 이를 감지하고 SA_TrapManager 모듈이 SA_COMM_TRAP 통신 모듈을 이용하여 마스터에게 웹 서버에 예외 상황이 발생했음을 알린다.



(그림 4) HTTP 에이전트 모듈 구조

3.4 SMTP 에이전트

SMTP 서비스 제공을 위해 관리 대상이 되는 메일 서버에서 동작하는 에이전트로, 트래픽 정보와 syslog 로그 파일 등의 다양한 정보를 수집 분석하는 역할을 한다. SMTP 에이전트의 주요 설계 모듈은 (그림 5)과 같으며 SA_Agent 모듈, SA_COMM 모듈, FileManager 모듈의 설계는 분석 대상이 되는 데이터만 다를 뿐 HTTP 에이전트의 설계 방식과 동일하다.



(그림 5) SMTP 에이전트 모듈 구조

① RequestAnalyer 모듈

RequestAnalyer 모듈은 마스터로부터 요청 받은 메시지를 분석하여 해당 처리 모듈을 호출하도록 설계되었다. 메일 서버의 syslog 로그 파일을 parcing 하는 SmtpAnalyer 모듈과 sendmail.st 파일이 생성된 이후 시간부터 일정 시간동안의 송/수신 메일에 관련된 정보를 분석하는 MailstatAnalyer 모듈을 호출하여 처리한 결과 값을 반환한다.

② LogFileManager 모듈

HTTP 에이전트의 모듈처럼 이기종의 메일 서버에서 획득한 syslog 로그 데이터의 관리를 위해 관리자가 설정한 데이터 포맷에 따라 로그 데이터를 파일 형태로 관리하는 모듈이다

③ SA_TrapManager 모듈

에이전트 시스템이 위치한 메일 서버의 트래픽과 로그 데이터 분석 동안 메일 사이즈가 관리자 설정 값을 초과하고, 계정에 없는 사용자가 메일을 보내는 일이 발생 하였을 경우 EventMonitor 모듈이 이를 감지한다. 그리고 SA_trpManager 모듈이 SA_COMM_TRAP 통신 모듈의 trap 메시지를 이용하여 마스터에게 메일 서버의 예외 상황을 알린다.

4. 서비스 관리 시스템 구현

4.1 주요 기능

자바 기술 기반의 서비스 관리 시스템은 사용자가 요구 하는 작업을 마스터와 해당 에이전트 시스템이 처리하여 결과 값을 반환하는 모듈화된 구조를 가지고 있으며 주요 기능은 다음과 같다.

- 로그 파일의 주기적 백업

  에이전트 시스템은 접속 로그, 에러 로그, 성능 로그, 추적 로그 데이터를 주기적으로 백업하여 중요 파일을 보존하고 에이전트와 마스터간의 로드 부하를 줄여 관리를 쉽게 한다.
- HTTP 서비스 제공

  웹 서버에서 제공하는 접속 로그 파일을 기반으로 월별 접속 현황 또는 시간대별 접속 현황 등의 접속 추이를 나타내어 데이터의 비교 분석을 용이하게 한다.
- SMTP 서비스 제공

  메일 서버의 syslog 과 mailstat 정보를 이용하여 시간별 혹은 사용자별 서비스 분석을 통해 효율적인 메일 서버의 운영을 돕는다.
- 에러 통계 및 분석

  로그 레벨별 분석을 통해 에러가 발생한 시간과 클라이언트 IP, 에러 정도, 에러 발생 이유 등을 분석하여 시스템의 안정화를 도모한다.
- 사용자 정책 설정

  사용자 관리 창을 통해 설정 권한을 줄 수 있으며, 사용자는 데이터 입력과 시스템의 동작을 제어하여 시스템의 전체 성능 향상을 돕는다.
- 에이전트 시스템 관리

  현재 마스터에서 관리하고 있는 에이전트 시스템들을 트리 형태의 정보로 제공하여 에이전

트별 통계 정보를 사용자가 쉽게 관리할 수 있다.

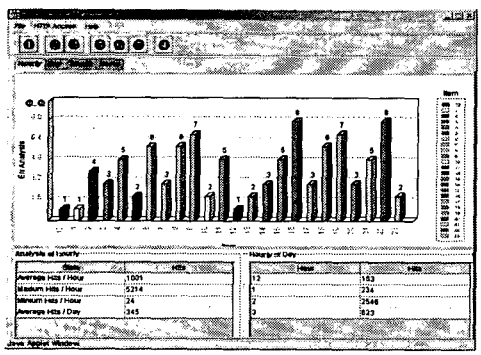
4.2 구현

본 논문에서 구현한 로그 분석을 통한 서비스 관리 시스템은 GUI 기반으로 서비스 이용자별 조회 현황과 접속 빈도가 높은 데이터의 통계가 가능하며 이를 통해 사용자 중심의 서비스 제공과 시스템 관리를 목적으로 한다.

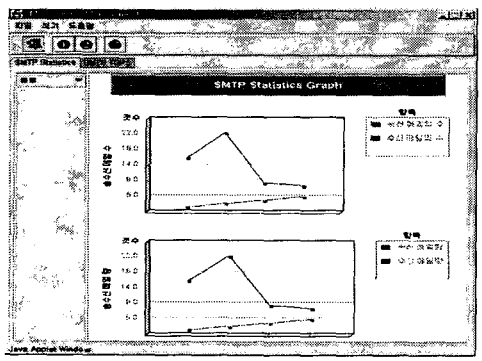
사용자 인터페이스는 각 에이전트에서 분석된 트래픽과 로그 데이터의 변화과정을 보여주고, 비교 분석을 용이하게 하기 위해서 그래프와 테이블과 같은 GUI 형태로 데이터의 분포도를 나타낸다. 각각의 인터페이스에는 사용자의 데이터 입력이나 동작 제어를 지원하는 정책 설정 패널이 존재하여 서비스 관리 시스템의 전체 성능 향상을 돕는다.

(그림 6)은 HTTP 서비스의 활용도와 성능을 높이기 위해서 웹 서버의 로그 데이터와 트랙픽 분석을 통해 웹 서버상에 얼마나 많은 접속이 이루어 졌는지 시간별, 일별, 월별, 호스트별 통계와 분석 자료를 제시한다.

(그림 7)은 메일 서버에서 제공하는 시스템 로그 데이터와 트래픽 분석을 통해 송/수신되는 메일의 개수와 크기(바이트 단위), 사용자별 메일 서비스 사용 통계와 시간대별 분석 정보의 변화 과정을 선 그래프로 나타내었다.



(그림 6) HTTP 서비스 통계



(그림 7) SMTP 서비스 통계

5. 결론 및 추후 연구 방향

인터넷의 보급과 대중화로 인해 사용자 수가 크게 증가하고 있으며 이에 따른 데이터양도 폭발적으로 증가하고 있다. 로그 파일에는 서버가 수행한 작업들에 대한 풍부한 정보가 들어 있으며, 이들은 단순히 특정 작업 요청과 성공 여부에 대한 것 뿐만 아니라 실패 했을 경우 그 해결책에 대한 정보도 들어있다.

본 논문에서는 이러한 로그 파일의 활용을 통해 서비스 관리 시스템의 모델을 제시하고 실제 구현을 통해 주요 기능 및 시스템의 특성을 살펴보았다,.

사용자의 요구 사항이 점점 복잡해지고 다양해짐에 따라 서비스의 품질을 향상시키고 개인화된 정보 제공을 위해서는 로그 데이터의 한계를 극복한 서비스의 특성에 맞는 지능화된 개인화 알고리즘을 개발해야 한다. 사용자 등록 정보, 외부 환경정보와 같은 추가적인 정보를 이용하여 사용자의 종합 특성을 도출해내는 능동적인 서비스 관리 시스템에 관한 연구도 필요할 것이다.

참고문헌

[1] Roger S. Pressman. "Software Engineering, A Practitioner's Approach", 3rd Ed. McGraw Hill, 1997

[2] 김석기, 언정용, 한경수, 한범수,"웹 로그 분석을 통한 정보의 활용", 한국통계학회 학술발표회 논문집, pp. 123-127, 2000

[3] 김광용, "Web Information Center 와 Internet Survey", Internet Survey Workshop 논문집, pp.111-122, 2000

[4] Garschhammer, M., Hauck, R., Hegering, H.-G., Kempter, B., Radisic, I., Rolle, H., Schmidt, H., Hegering, H.-G., Langer, M., Nerb, M., " Towards generic service management concepts a service model based approach", Integrated Network Management Proceedings, pp. 719 -732, 2001.

[5] Chang-Jiun Tsai, Tseng, S.S., Sheng-Hui Chen, " Design and implementation of a personalized service management system", Systems, Man, and Cybernetics, Vol. 1 , pp. 542 - 547, 2000.

[6] Croll, M., Lee, A., Parnall, S., " Content management-the users requirements", Broadcasting Convention, 1997. IBS 97., International (Conf. Publ. 447) , pp. LP6 -LP9, 1999.

[7] HeaSook Park, O-Hoon Choi, Doo-Kwon Baik, " CORBA based approach to the development of an advanced architecture in TINA service management system", Database and Expert Systems Applications, Proceedings. pp. 175 -179 , 2001.