SNMP 기반 네트워크 관리를 위한 적응형 네트워크 모니터링 방법

정회원 천 진 영*, 정 진 하*, 윤 완 오*, 최 상 방*

Adaptive Network Monitoring Strategy for SNMP-Based Network Management

Jin-young Cheon, Jin-ha Cheong, Wan-oh Yoon, Sang-bang Choi *Regular Members*

요 약

네트워크 관리시스템에서는 SNMP를 기반으로 하는 중앙 집중형 방법과 모빌 에이전트를 사용하는 분산형 방법으로 나눌 수 있다. 네트워크 정보가 시간에 따라 변하는 경우 매니저는 실시간으로 이를 관찰할 필요가 있으며, 이 경우 SNMP에서는 매니저가 주기적으로 에이전트에 질의를 보낼 수 있어 주로 폴링을 사용한다. 그러나 폴링에서는 정보 전송을 위해서 매번 요구와 응답의 두 메시지 전송이 필요하여 네트워크 트래픽이 증가한다. 본 논문은 SNMP 기반 네트워크 관리에서 기존의 폴링 방법과 비교하여 트래픽을 줄이면서 여러 에이전트를 충실히 모니터링할 수 있는 적응형 방법을 제안하였다. 제안된 방법에서는 각 에이전트가 정보의 시간적 변화량에 따라 최적의 에이전트 모니터링 주기를 결정하고, 매니저는 이 주기들을 취합하여 모니터링에 의한 부하가 전체 네트워크 트래픽의 일정 부분 이하가 되도록 모니터링 주기를 결정한다. 에이전트는 매니저로부터 받은 모니터링 주기에 따라 스스로 정보를 전송함으로써 기존의 폴링 방법보다 상대적으로 적은 트래픽 부하로 네트워크 관리가 가능하다. 제안된 방법의 성능을 평가하기 위하여 그 기능을 구현하였으며, 모니터링의 충실도와 트래픽 면에서 일반적인 폴링방법과 비교하였다.

ABSTRACT

In the network management system, there are two approaches; the centralized approach based on SNMP and the distributed approach based on mobile agent. Some information changes with time and the manager needs to monitor its value in real time. In such a case, the polling is generally used in SNMP because the manager can query agents periodically. However, the polling scheme needs both request and response messages for management information every time, which results in network traffic increase. In this paper, we suggest an adaptive network monitoring method to reduce the network traffic for SNMP-based network management. In the proposed strategy, each agent first decides its own monitoring period. Then, the manager collects them and approves each agent's period without modification or adjusts it based on the total traffic generated by monitoring messages. After receiving response message containing monitoring period from the manager, each agent sends management information periodically without the request of manager. To evaluate performance of the proposed method, we implemented it and compared the network traffic and monitoring quality of the proposed scheme with the general polling method.

* 인하대학교 전자공학과 컴퓨터구조 및 네트워크 연구실(sangbang@inha.ac.kr)
논문번호 : 020369-0824, 접수일자 : 2002년 8월 24일
※ 이 논문은 2002년도 인하대학교 지원에 의하여 연구되었음. (INHA-22767)

Ⅰ. Introduction

An efficient and automated network management is required in large and complex networks since it is very difficult to manage them only with human effort. In the network management system, there are two approaches in general; the centralized approach based on SNMP (Simple Network Management Protocol) and the distributed approach based on mobile agent. In the network monitoring of SNMP, network elements accumulate network management information and send it to the manager using polling and event reporting. The polling is a request-response interaction for management information between the manager and the managed agent. Whereas, in event reporting, the manager is just listening to incoming management information from agents. And each agent sends the information whenever it needs to do so based on its decision[1,2].

Since some agent information changes with time, the manager should monitor and control the network resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost. To convey the MIB (management information base), the polling is generally used in SNMP since the manager can query agents periodically. However, if polling is performed frequently, the traffic of management information can become excessively high. In contrast, if the polling frequency is low, the manager may not be able to keep track of the variation of management information faithfully. There is always a trade-off between the monitoring quality and extra traffic needed in polling. Thus, appropriate monitoring frequency should be determined with which the manager can monitor agents without loss of the management information. However, as described before, polling needs one pair of request and response messages for every information and can generate heavy message traffic.

In this paper, we suggest a new dynamic monitoring strategy to reduce the message traffic in SNMP-based network management. In the proposed method, each agent first decides its own monitoring period. After the agents decide their monitoring periods, the manager collects them and calculates the total amount of monitoring traffic assuming that each agent may send information with the frequency of its own monitoring period. If the total traffic doesn't exceed an allocated network bandwidth, which is predetermined by a network administrator, the manager approves each agent's monitoring period. Otherwise, the manager adjusts the period using the negotiation factor (NF) and notifies the modified period to each agent. Finally, each agent sends network information using the received monitoring period. We have implemented the proposed adaptive monitoring method, and compared the network traffic and monitoring quality of proposed scheme with the general polling method.

The rest of the paper is organized as follows. In Section 2, we describe the general polling method used in SNMP and its drawbacks. In Section 3, we explain the proposed network monitoring method for faithful network management. In Section 4, we discuss the implementation of the proposed method, and compare the network traffic and monitoring quality of the implemented method with the general polling scheme. Finally, we give concluding remarks and discuss the future works in Section 5.

Ⅱ. SNMP and Network Monitoring

2.1 SNMP

To manage the complex network within a coherent framework, SNMP has been developed and adopted for TCP/IP internet as a standard protocol[1]. The SNMP network management has two functional categories, which are network monitoring and network controlling[2]. The network monitoring is concerned with observing and analyzing the status and behavior of the network configuration elements, and the network controlling is concerned with modifying

parameters and invoking actions to be taken by the network configuration elements. In SNMP, a network management station is designated as a manager to monitor and control the network and a managed network element, which is called an agent, responds to requests from the manager. There may be more than one manager in the network. However, we assume only one manager without loss of generality in this paper.

Information that is useful for network monitoring is gathered and stored by agents and made available to one or more manager systems. Two techniques are used to make the agent information available to the manager; polling and event reporting. The polling is a request-response interaction between the manager and agent. The manager can query any agent (for which it has authorization) and request the values of various information elements; an agent responds with information matching certain criteria, or supplies the manager with information about the structure of the MIB. The manager system may use polling to learn about the network configuration it is managing, to periodically obtain a change of conditions, or to investigate an area in detail after being alerted by a problem. Polling is also used to generate a report on behalf of a user and to respond to specific user queries.

In SNMP, the manager and agents send and receive five types of messages i.e., get-request, get-next-request, set-request, get-response and trap[2]. In the polling method, the manager sends get-request or get-next-request message when it requests agent information during a polling period and then the agent sends get-response message for the manager's request. Those five types of messages between manager and agent and communication ports for each messages are depicted in Figure 1.

2.2 Polling for Network Monitoring

In the general polling scheme, the manager can request only one agent for management information.

It can't poll any other agent until get-response

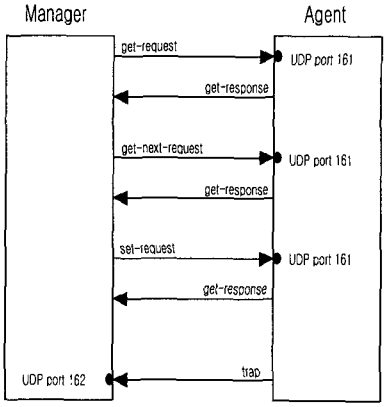


Fig. 1 SNMP messages and operations

message is requested agent. Thus, the polling period T_{delay} (the time between two successive polling requests to the same agent) must satisfy following condition.

$$T_{delay} \geq (\Delta \times N), \tag{1}$$

where Δ is the minimum time required for the manager to receive a response message successfully from the agent for a request of management information, and N is the total number of agents. The network manager's polling period T_{delay} for each agent is limited by the above equation.

We must consider another condition from a network traffic point of view. The network traffic caused by polling should be kept below a certain portion of the possible bandwidth of an underlying network since the network has to be used for other application processes[3]. The allowed traffic for network monitoring would be predefined by the network manager. The following equation shows the minimum polling period $T_{traffic}$ determined by the traffic of network management messages with respect to an allocated bandwidth.

$$T_{traffic} = \frac{\sum(\text{Network Traffic for Each Polling})}{(\text{Allocated Network Bandwidth})} \tag{2}$$

To monitor agent's management information in

real time, the manager should choose the polling period to be at least twice the maximum variation frequency f_{max} of the monitored value[4]. This is based on the well-known Shannon sampling theorem. The maximum variation frequency f_{max} can be directly calculated through DFT (Discrete Fourier Transformation). Thus, we can determine the minimum polling period T_{sample} to monitor each agent without loss of any information from the following equation.

$$T_{sample} = \frac{1}{2 \times f_{max}} \quad (3)$$

The above conditions present guideline to determine a polling period considering network delay, network traffic, and variation of monitored value to keep track of each agent's management information without any loss. The following equation shows lower and upper limits of polling period $T_{polling}$ for the manager to fully monitor the network.

$$T_{sample} \geq T_{polling} \geq \text{Max}\{T_{delay}, T_{traffic}\} \quad (4)$$

However, polling needs both request and response messages for management information at every time. Thus, in the polling, the management message traffic becomes excessive to manage a network appropriately when there are many network elements contained in the network. In the following section, we explain the proposed monitoring method to reduce the management message traffic for SNMP-based network management.

Ⅲ. Adaptive Network Monitoring Strategy

3.1 Proposed Monitoring Method

In the proposed method, when mutual agreements are made between manager and agents, each agent sends management information in its own period without the manager's participation. Thus, the proposed method obtains a merit of periodical polling without the manager's requests in network monitoring.

First of all, each agent decides its own monitoring period from the time variation of values of management information. We define this period as the Agent Monitoring Period (AMP) in

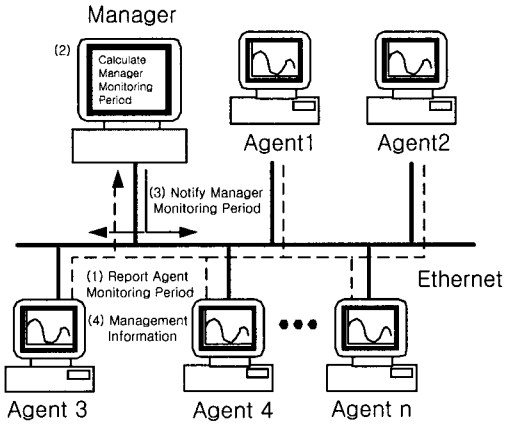


Fig. 2 Message flows between the manager and agent in the proposed method

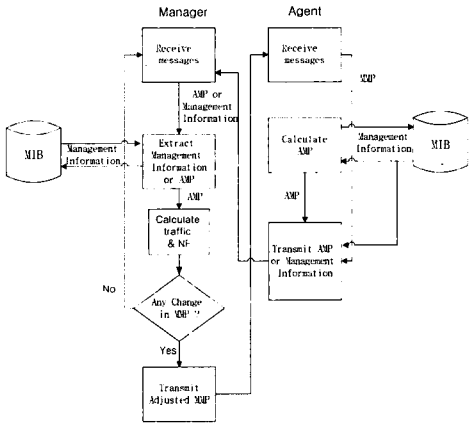


Fig. 3 Operation flows of the manager and agent in the proposed method

this paper. Then, each agent sends a message containing a calculated AMP to the manager. The manager collects the AMPs and adjust them such that total traffic is less than an allocated network bandwidth. We define this adjusted period as the Manager Monitoring Period (MMP). And the manager notifies the MMP to each agent. Then, each agent sends management information according to the received MMP. Figure 2 shows

a flow of messages between the manager and agents in the proposed monitoring strategy. When an agent has to send management information using a period different from the received MMP some time later, it reports a new AMP to the manager. The manager continues to collect new AMPs from agents and recalculates appropriate MMPs for each agent. If a new calculated MMP is different from the previous MMP by a certain level, the manager notifies the new MMP to the corresponding agent. Figure 3 shows the general operation flows of the manager and agent in the proposed scheme. Detailed explanations are given in the following two subsections. The UDP is employed to transport messages between the manager and agents.

3.2 Agent Monitoring Period

In an organization, the network monitoring job for the MIB information is concerned with observing and analyzing the status and behavior of the end systems, intermediate systems, and sub-networks that make up the configuration to be managed. Before considering the design of a network monitoring system, it is the most important to determine the types of monitored data that are of interest to a network management.

The information that should be available for network monitoring can be classified as follows.

Static: It is the information that characterizes the current structure and the elements in the current configuration such as the number and identification of ports on a host or router. This information will change infrequently.

Dynamic: This information is related to events in the network, such as a state change of network element or the transmission of packets on the network.

Statistical: It is the information that can be derived from the dynamic information such as the average number of packets transmitted per unit time by an end system.

The dynamic information must be collected within a certain time interval from the monitored network elements because it varies with time and the statistical information is obtained from it. Thus, it is important for the manager to keep track of the time variation of the dynamic network information from values that are sampled and reported by agents.

Depending on the types and time properties of the agent information, each agent can determine AMP with various methods. In theory, the AMP should be the reciprocal of at least twice its maximum frequency f_{max} of the time variation of management information. And the maximum frequency f_{max} of an management information is derived through the DFT calculation. However, it is not easy to extract exact f_{max} from the information in real environment. Thus, the amplitude of frequency component that is larger than 2% of the maximum value is considered as a valuable frequency f'_{max} to filter out high frequency jitter of values, and then use twice the frequency $2f'_{max}$ as a sampling rate in our implementation. The main point of the proposed scheme is to reduce extra traffic needed to monitor the network faithfully without suffering from any loss of significant management information.

3.3 Manager Monitoring Period

The manager collects reported AMPs and calculates the total traffic assuming that each agent sends management information using its AMP. If the traffic generated by network monitoring messages is below a certain level of network bandwidth, which is preset by a network administrator, the manager approves reported AMPs and sends them as MMPs without any modification. However, if the total traffic does not satisfy the allocated bandwidth, the manager lengthens the AMPs proportionately to determine MMPs. If the reported AMPs are extended beyond a certain ratio, we cannot expect to fully monitor the network.

The network administrator decides how to allocate and restrict network bandwidth for the

network management. He can restrict the management traffic using an absolute quantity or using a relative ratio of total bandwidth empirically. In general, the traffic for network management is restricted below 15% of total bandwidth[1,3,5].

The expected traffic generated by management messages can be calculated by the following formula[6].

$$Expected\ traffic = \sum(PS_1/AMP_1 + \cdots + PS_n/AMP_n) \quad (5)$$

where PS_i is an average size (number of bits) of messages to transport management information from agent i and n is the number of agents. If the manager predicts that the expected traffic of management message is larger than that of an allocated bandwidth, it calculates a Negotiation Factor (NF) as follows.

$$NF = \frac{\sum(PS_1/AMP_1 + \cdots + PS_n/AMP_n)}{Allocatea\ Network\ Bandwidth} \quad (6)$$

The manager obtains MMPs from multiplying received AMPs by the NF as follows.

$$\begin{aligned} MMP_1 &= NF \times AMP_1 \\ MMP_2 &= NF \times AMP_2 \\ &\cdots \\ MMP_n &= NF \times AMP_n \end{aligned} \quad (7)$$

The five types of messages used in the SNMP are get_request, set-request, get_next-request, get-response, and trap as explained in Section 2.1. In our implementation, the trap message is used to send AMPs and management information from agents to the manager. And the set-request message is used to send MMPs to each agent. Figure 4 shows message formats to send or receive several pairs of Object Identification (OID) and the corresponding value for the network management[1,7].

In the proposed method, we use specially designed PDU type 5 to send MMPs simultaneously using broadcast. Figure 5 is a new message format for the type 5. We write the IP address of an agent in the OID field and write an MMP for the agent in its value field. Using this format, we can broadcast several MMP values to reduce management message traffic rather than notifying each agent using an individual message. Each agent can extract its MMP value using IP address without any difficulty.

We also change the general SNMP trap message for each agent to report its AMP value and management information to the manager as shown in Figure 6. The first OID represents AMP and the value is written in the second field. Remaining fields are used for reporting values of interesting variables for network management.

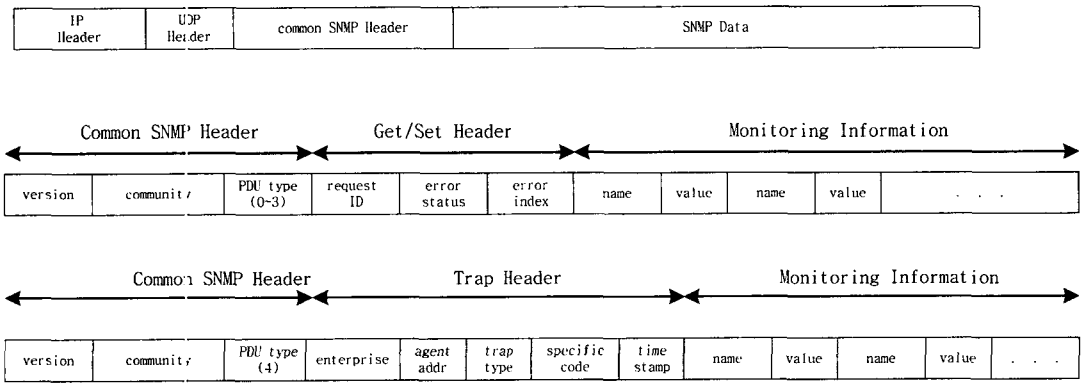


Fig. 4 SNMP message format

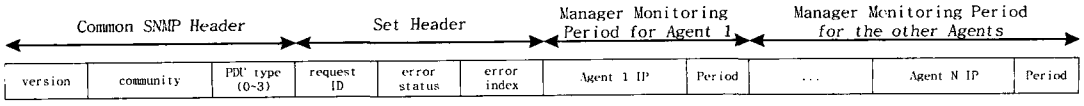


Fig. 5 Manager message format

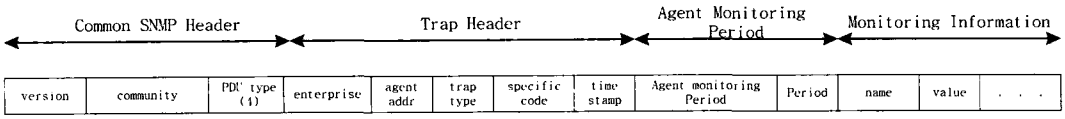


Fig. 6 Agent message format

Ⅳ. Implementation

4.1 Implementation Environment

We have implemented the proposed network management method and made several experimentations to evaluate the quality of network monitoring and the performance of the proposed method. In the first experiment, we tested our implementation in a simple network configuration, i.e., we employed one server (Windows NT) as the manager and 4 PCs (Windows 98) as agents. In the second experiment, the network monitoring was performed in a larger network configuration using 16 PCs. All hosts are connected to 10BaseT Ethernet. In the experiments, the CPU utilization is monitored for busy hosts. In each host, the CPU utilization has a value between 0 and 1 and varies in time. And one time unit is equal to two seconds in the following description and graphs. The general polling method is also carried out to compare the performance of the proposed scheme.

Two metrics were used to evaluate the performance and quality of network monitoring. First, the network traffic is measured to compare the amount of management messages generated by the network monitoring. Next, we evaluate the faithfulness of monitored values of agent's information. We calculate and compare the average deviations of agent's original values and monitored values. In this experiment, the average deviation to evaluate the faithfulness of monitored value is defined by the following formula.

$$\textit{Average deviation} = \frac{(|M_1 - A_1| + |M_2 - A_2| + \cdots + |M_t - A_t|)}{t} \tag{8}$$

where t is the time (seconds) spent since the network monitoring starts. A_i, $i = 1, 2, \ldots, t$, is the agent's original value at time i. And M_i, $i = 1, 2, \ldots, t$, is a value that is kept by the manager at time i. When the manager receive a value v_1 from an agent at time t_1, the value v_1 is kept as M_{t_1} until another value v_2 is received at time t_2 as follows.

$$\begin{aligned} M_{t_1} &= M_{t_1+1} = \cdots = M_{t_2-1} = v_1 \\ M_{t_2} &= v_2 \end{aligned} \tag{9}$$

For example, when the manager receives $v_1 = 0.6$ at $t_1 = 4$ and $v_2 = 0.9$ at $t_2 = 7$, then $M_4 = M_5 = M_6 = 0.6$ and $M_7 = 0.9$.

In the experiments, each agent extracts frequency components by applying DFT for 180 seconds. The amplitude of frequency component that is larger than 2% of the maximum value is considered as a valuable frequency. Then, the highest frequency among them is regarded as f_{max} and the AMP for the corresponding management information is set to $1/(2 \cdot f_{max})$. And the agent's minimum monitoring frequency is

restricted above 0.001 Hz. As an upper limit of monitoring frequency, we use extra traffic generated by management message and limit the traffic to be maintained below 800 Bytes/Min.

4.2 Experiment

In the first experiment, a small network configuration is used to verify the implementation and to get some insight into the network management operation under the given environment. That is, one manager and four agents are connected to the Ethernet. The manager and each agents record management information values and network traffic for 60 minutes in each experiment. After running the general polling method and the proposed method to monitor a given network, the average deviations of agent's information values and monitored values are compared. And the network traffic produced by each monitoring method is also compared in each case.

Figure 7 depicts the variation of management information values in an agent that is randomly selected among four agents. And the corresponding agent's AMPs, which are calculated by applying DFT to the values, are shown in Figure 8.

In this network configuration, the network traffic generated by management messages is not excessive because of the small number of agents. Thus, AMPs that each agent sends are accepted without modification by the manager throughout the experiment. The agent reports the values 27 times during the experiment. To make a fair comparison, the manager uses equally spaced polling in time and makes 27 requests, i.e., at every 133 seconds (3600/27) during the entire experiment period. Note that the proposed method uses adaptive periods that change in time with the variation of the monitored values in time with the variation of the monitored values rather than a fixed time interval.

The differences between the agent's original values and the manager's received values are shown in Figures 9 and 10 for the proposed

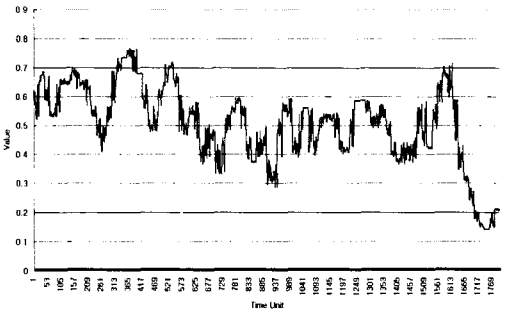


Fig. 7 Time variation of an agent's CPU utilization in the first experiment

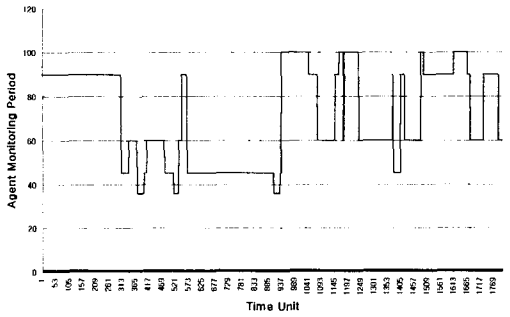


Fig. 8 Time variation of an agent's monitoring period in the first experiment

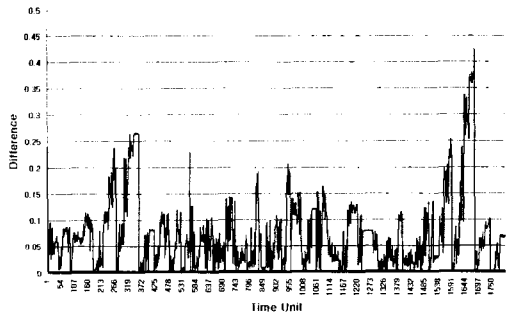


Fig. 9 Differences between the agent's original values and the manager's received values when the proposed method is used in the first experiment

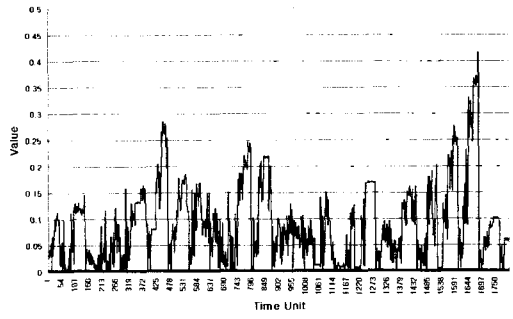


Fig. 10 Differences between the agent's original values and the manager's received values when the general polling method is used in the first experiment

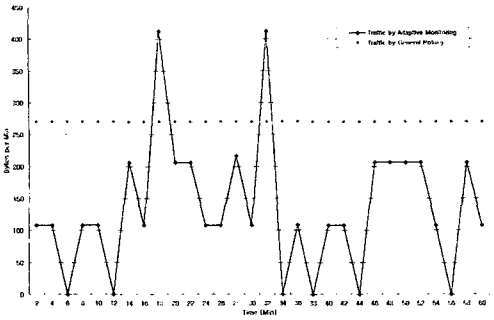


Fig. 11 Network traffic caused by management messages in the first experiment. Note that the traffic generated the polling method is constant in time

scheme and the polling method, respectively. Average deviations between the agent's original values and the manager's received values are 0.043 and 0.088 for the proposed method and the general polling, respectively, in this experiment. Even though the network used in the experiment contains only four agents, the quality or faithfulness of the proposed scheme in monitoring agents is obviously better when compared with the polling method.

Fig. 11 shows two graphs of management message traffic, which is generated by each of two monitoring methods. Note that the traffic generated by the polling method is constant throughout the experiment. In terms of induced network traffic, the proposed monitoring method is superior to the polling method.

In the second experiment, we use a larger network configuration with 16 PCs. In this

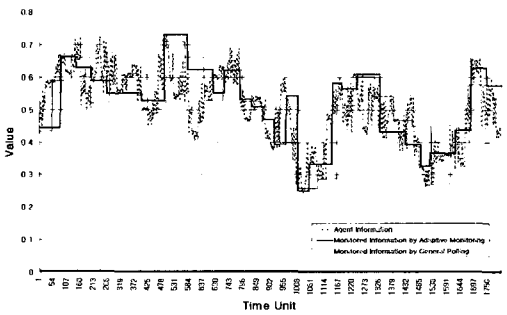


Fig. 12 Variation of management information values over time. The values are sent by the Agent 1 when the proposed method is used in the second experiment

subsection, the data obtained from randomly chosen 4 agents, which are denoted as agents 1 through 4, are presented. Figures 12 through 15 show the variation of management information values over time for each agent.

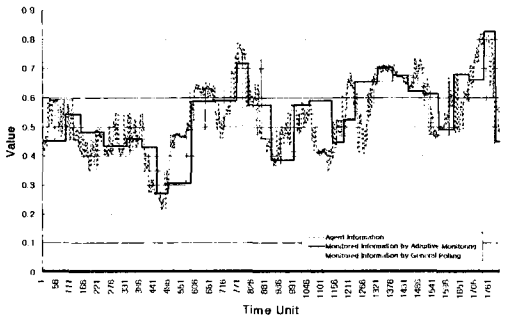


Fig. 13 Time variation of monitored information values that are sent by the Agent 2

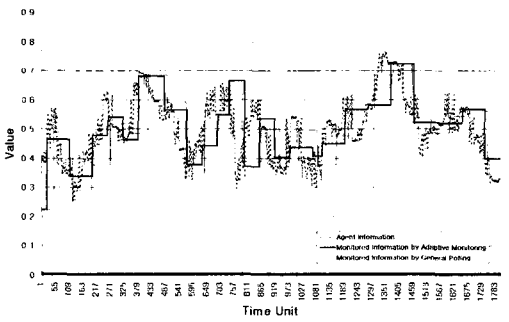


Fig. 14 Time variation of monitored information values that are sent by the Agent 3

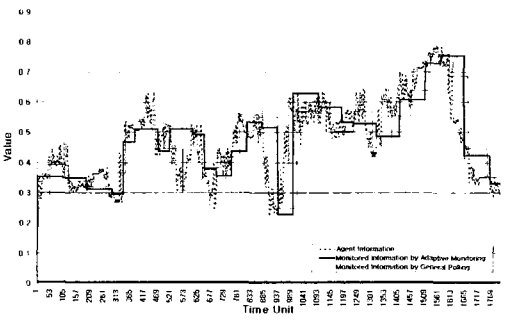


Fig. 15 Time variation of monitored information values that are sent by the Agent 4

In the large network configuration, it is not obvious whether the proposed method can keep track of monitored values more faithfully than the polling method from the above four figures.

However, the quality of the proposed scheme in monitoring agent's information values is definitely superior when the average deviation and network traffic are compared. Table 1 shows average deviations of monitored values obtained from the two monitoring methods in the second experiment. Figure 16 depicts the network traffic created by the proposed adaptive monitoring method and the general polling. The traffic of the proposed method is reduced to 71% of the polling method. If the time period is lengthen to reduce the traffic of the general polling method, the average deviation becomes worsen significantly. From the two experiments, we can observe that the proposed monitoring method provides excellent performance in terms of both monitoring faithfulness and network traffic in managing the network.

Table 1. Average deviations between the agent's original values and the manager's received values

	Agent 1	Agent 2	Agent 3	Agent 4
Adaptive Monitoring	0.03681	0.04462	0.04729	0.04473
General Polling	0.04512	0.04919	0.06337	0.05154

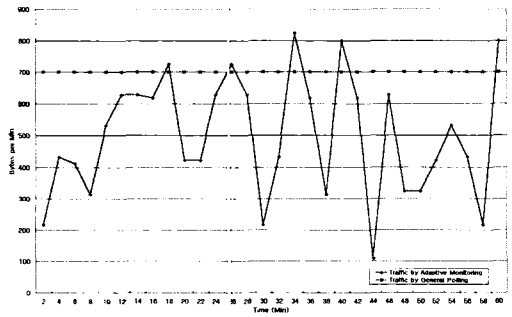


Fig. 16 Network traffic of proposed adaptive monitoring method versus polling method

V. Conclusion

For management information that varies with time, the polling is generally used in SNMP since the manager can query agents periodically in this technique. However, the polling can create much traffic since it needs both request and response messages for each management information.

In this paper, we present an adaptive network monitoring strategy to reduce the network traffic for SNMP-based network management. In the proposed strategy, each agent decides its AMP and reports it to the manager. Then the manager collects them, and approves the AMPs without modification or adjusts them depending on the relative management traffic compared to the network bandwidth. Agents send management information periodically using received MMPs without the request of manager.

To show the superior performance of the proposed method, we implement it and performed two kinds of experiments. One experiment is performed in a small network configuration and the other experiment is done in a much larger network to compare the network traffic and average deviations of monitored values. From the two experiments, we can see that the proposed adaptive monitoring method provides excellent performance in terms of both monitoring faithfulness and network traffic for network management. As a future search, we will employ two ore more manager systems in the network configuration. Hierarchical network management structures will be also considered to expand and improve the monitoring functions of our implementation in real network environment.

References

[1] W.R. Stevens, *TCP/IP Illustrated*, Volume1: The Protocols, Addison Wesley, 1994.

[2] W. Stallings, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*: 2nd Edition, Addison Wesley, 1999.

[3] K.C. Hwang, "A SNMP Group Polling for the Management Traffic," *Proceedings of IEEE TENCON* '99, vol. 2, pp. 797-800, Sept. 1999.

[4] K. Yoshihara, K. Sugiyama, H. Horiuchi, and S. Obana, "Dynamic Polling Algorithm Based on Network Management Information Values," *IEICE Trans. commun.*, vol. E82-B, no. 6, pp.

868-876, June 1999.

[5] M. Cheikhrouhou, and J. Labetoulle, "An Efficient Polling Layer for SNMP," *Network Operation and Measurement Symposium*, pp. 477-490, April 2000.

[6] M. Aron and P. Druschel, "Soft Timers: Efficient Microsecond Software Timer Support for Network Processing," *ACM Trans. on Computer Systems*, vol. 18, no. 3, pp. 197-228, August 2000.

[7] Y. Guo, "Hierarchical Network Management Based on Extended SNMP," *Transaction of IEE of Japan*, vol. 119-c, no. 3, pp. 404-412, 1999.

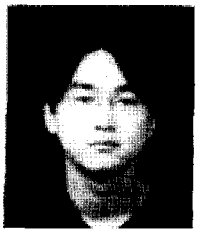
천 진 영(Jin-young Cheon)

1998년 3월 : 인하대학교 전자공학과 졸업
2001년 8월 : 인하대학교 전자공학과 석사
2001년 8월~현재 : LG전자연구소 SIC연구센터 주임연구원
<주관심 분야> 컴퓨터 구조 병렬처리, 컴퓨터 네트워크

정 진 하(Jin-ha Jung)

1992년 2월 : 인하대학교 전자공학과 졸업
1994년 2월 : 인하대학교 전자공학과 석사
1994년 2월~1999년 12월 : (주) 한미기술연구소
2000년 3월~현재 : 인하대학교 전자공학과 박사과정
<주관심 분야> 컴퓨터 구조 병렬처리, 컴퓨터 네트워크

윤 완 오(Wan-oh Yoon)



2000년 2월 : 경기대학교 전자공학과 졸업
2002년 2월 : 인하대학교 전자공학과 석사
2002년 3월~현재 : 인하대학교 전자공학과 박사과정
<주관심 분야> 분산 처리 시스템, 병렬프로그래밍, 컴퓨터 아키텍처

최 상 방(Sang-bang Choi) 정회원

1981년 2월 : 한양대학교 전자공학과 졸업
1981년~1986년 : LG 정보통신(주)
1988년 3월 : University of Washington 석사
1990년 8월 : University of Washington 박사
1991년~현재 : 인하대학교 전자공학과 교수
<주관심 분야> 컴퓨터 구조, 컴퓨터 네트워크, 병렬 및 분산 처리 시스템, Fault-tolerant computing