이동 IP 망에서의 DMSP 핸드오프를 위한 멀티캐스트 방안

Multicast Schemes for DMSP Handoff in Mobile IP Networks

남 세 현*
Seahyeon Nam

요 약

본 논문에서는 이동 멀티캐스트(MoM) 프로토콜에서 DMSP 핸드오프로 인하여 발생하는 패킷 손실 문제를 여러 DMSP 선택 방식에 대하여 모의실험을 통하여 조사하였다. 모의실험 결과로 한 개의 DMSP를 갖는 MoM 프로토콜에서는 상당한 패킷 손실이 발생하는데 이를 최소화하기 위하여 두 가지 향상된 멀티캐스트 방안을 제안한다. 제안된 첫 번째 방안은 백업 DMSP를 사용하여 망 내부에서의 트래픽은 증가하지만 패킷 손실율을 크게 줄일 수 있는 방안이다. 제안된 두 번째 방안은 확장된 DMSP 기능을 추가하여 망 내부에서의 트래픽도 낮게 유지하면서 동시에 패킷 손실율을 최소화하는 방안이다.

Abstract

The packet loss problem that occurs in the mobile multicast (MoM) protocol due to designated multicast service provider (DMSP) handoff is investigated through simulation experiments for several DMSP selection policies. Then, two enhanced DMSP schemes are proposed to minimize the packet loss of the MoM protocol with single DMSP. The first scheme uses a backup DMSP and greatly reduces the packet loss rate at the expense of the increased network traffic. The second scheme utilizes the extended DMSP operation and shows many desirable features such as the almost zero packet loss rate and relatively low network traffic.

☞ Keyword : mobile IP, multicast, packet loss

I. Introduction

Multicasting for mobile hosts in an IP network is a challenging task. The addition of mobility in the host group model implies that the multicast forwarding algorithm ought to focus not only on the issue of dynamic group membership, but also on host location. In wireless mobile networks, the bandwidth is limited, wireless links are error-prone, mobile hosts frequently handoff, and battery lifetime of a mobile device is limited. Thus, when we design a multicast routing protocol for wireless mobile networks, the characteristics mentioned above should be carefully considered. Several multicast routing protocols for wireless mobile networks have been proposed [1]-[9]. Although the protocols solve several problems inherent in multicast routing proposals for static hosts, they still have problems such as non-optimal delivery path, lost packets due to handoff, and etc.

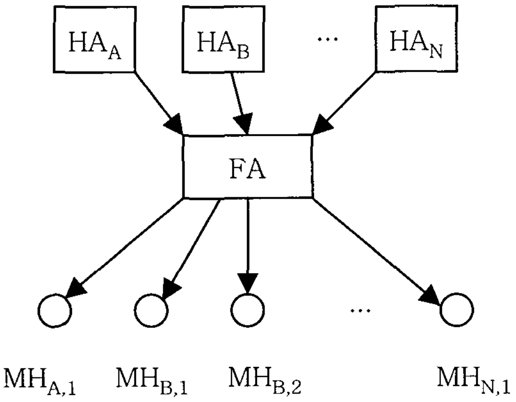
Two basic mechanisms have been proposed by the IETF in Mobile IP [1] to support multicasting. These are known as remote subscription and bi-directional tunneling. In re-

---

* 정 회 원 : 대구대학교 정보통신공학부 교수
shnam@daegu.ac.kr
[2004/07/09 투고 - 2004/10/08 1차 - 2005/02/02 2차 - 2005/05/04 심사완료]

mote subscription, the mobile host (MH) re-subscribes to the multicast group each time it moves to a new foreign network. It is the simplest way of providing multicast through Mobile IP. There is no special encapsulation needed, and it works well with basic Mobile IP. However, this approach is not suitable for highly mobile users since frequent resubscription in each foreign network may lead to lost packets. Moreover, frequent reconstruction of the multicast delivery tree may result in substantial control overhead.

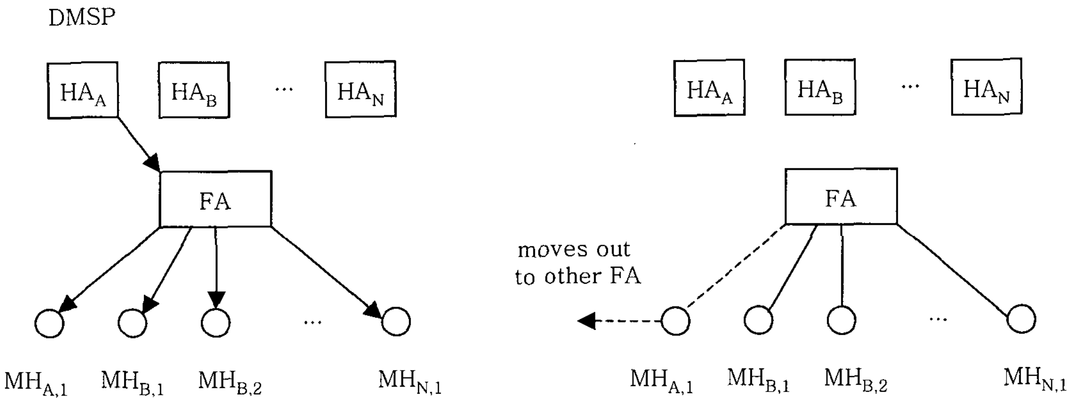
In bi-directional tunneling, the MH sends and receives multicast packets by way of its home agent (HA) using the unicast Mobile IP tunnels. This approach hides host mobility from all other members of the group. Since packets are forwarded from the HA, there is no need of updating the multicast delivery tree due to the MH movement. The main drawback of this approach is the routing path for multicast packet delivery that can be far from optimal. In addition, the HA must replicate and deliver tunneled multicast packet to all its MHs, regardless of at which foreign networks they reside. When many MHs, belonging to different HAs, move to the same foreign agent (FA), each of the respective HAs creates a separate tunnel to the FA so that multicast packets to their respective MHs can be forwarded. If these MHs were subscribed to the same group, all of the tunnels from different HAs to the FA would carry the same multicast packet, resulting in packet duplication. This is called the tunnel convergence problem (see Fig. 1).



〈Fig 1〉 Tunnel convergence problem

MoM [2] addressed the tunnel convergence problem by selecting only one HA among the given set of HAs. The selected HA among the given set of HAs is called designated multicast service provider (DMSP). However, this scheme may result in packet loss if the MH belonging to the currently serving DMSP moves out. This temporary multicast service outage stems from the fact that in Mobile IP there is no explicit deregistration with the FA when a host moves out. The MH's HA learns of the movement when the MH reregisters at the new network, but the FA at the old foreign network learns about the movement only through a timeout. In the case that the moving host's HA was the DMSP for a group at the previous foreign network and it was the last MH from the HA, a DMSP handoff will be required to a different HA to forward multicast packets for the remaining multicast group members at the foreign network. Until this DMSP handoff completes, multicast packet delivery for group members at the foreign network may be disrupted (see Fig. 2).

The Range-Based Mobile Multicast (RBMoM) protocol has been proposed in order to trade off between the shortest delivery path and the



(a) HAA is the DMSP at EA. (b) No DMSPs:multicast services are disrupted.

〈Fig 2〉 DMSP handoff problem

overhead induced by the multicast delivery tree reconfiguration [3,4]. It selects a router, called a multicast HA (MHA), which is responsible for tunneling multicast packets to the FA to which the MH is currently subscribed. The MHA can only serve MHs that are roaming around foreign networks and are within its service range. If a MH is out of service range, MHA handoff will occur. Therefore, this protocol has the packet loss problem due to the MHA handoff. Moreover, this protocol requires that each MHA be a multicast group member. A similar protocol has also been proposed in [5]. It is called Multicast by Multicast Agent (MMA) and introduces a multicast agent (MA) and a multicast forwarder (MF). Like the MHA in RBMoM, an MF is responsible for forwarding multicast packets to the MA of the foreign network, but in MMA the range of the MF is unlimited.

For the Mobile IPv6 environment, an enhanced version of the RBMoM protocol was proposed in [6] and [7]. To determine an optimal service range and avoid service disruption, this approach uses the RSVP signaling mechanism and introduces additional entities. The service range is defined as the maximum tunneling path length tolerated from the multicast source and is maintained by the core source node (CSN). The dynamic service range is defined as the maximum tunneling path length that satisfies the maximum tolerable transfer delay and is maintained by each MHA. To avoid long service disruption times, this approach employs the RSVP protocol and defines the boundary foreign agent (BFA). Compared to the RBMoM, this approach reduces the number of multicast tree reconstructions and multicast service disruption time. However, movement prediction and discovery of additional entities by the mobile receiver are the major problems. Moreover, this solution is not compatible with existing multicast membership protocols. A far as the application field is concerned, this solution seems to be suitable for intolerant and time-sensitive multicast applications, which need an absolute bound on multicast packet delay.

The Timer-Based Mobile Multicast (TBMoM) [8] protocol was proposed to find the tradeoff between providing low tree reconstruction overhead and fast data delivery to mobile nodes. When a mobile receiver moves fast passing many foreign networks in a relatively short time, it is served with fast unicast tunneling between foreign multicast agents (FMAs). Otherwise, the local FA joins the multicast group in a similar manner as in the remote subscription approach. Compared to the remote subscription approach, the TBMoM protocol reduces multicast packet loss and tree reconfiguration overhead. However, it introduces complex data structures and depends on the speed of the mobile members. In addition, the optimal join timer is not fixed since it depends on many parameters such as network topology, handover latency, and the speed of the mobile nodes.

Explicit multicast (Xcast) [9] is a new scheme for Internet multicast that complements the traditional multicast schemes. In the Xcast, the source node keeps track of the destinations in the multicast session. Whereas the traditional multicast schemes can support a limited number of very large multicast sessions, the Xcast can support a very large number of small multicast sessions. In general, xcasting is more efficient than unicasting because a single packet can hold data intended for multiple destinations, but it is less efficient than traditional multicasting because the addresses of these multiple destinations must be encoded in each packet, and the maximum packet size in the network limits the number of destinations that a packet may have. Therefore, xcasting was considered as an alternative solution to traditional multicasting that excels at handling data being sent to small number of destinations.

In this paper, the packet loss problem due to DMSP handoff in MoM protocol is investigated through simulation experiments for several DMSP selection policies. Then, two multicast delivery schemes are proposed to minimize the packet loss that occurs in the MoM protocol with single DMSP during DMSP handoff and relocation. The proposed schemes utilize a backup DMSP or an extended DMSP operation. These schemes greatly reduce the packet loss rate at the expense of the increased network traffic or the extra protocol overhead related to the operation of the extended DMSP.

The remainder of this paper is divided as follows. The proposed two schemes to minimize the packet loss during DMSP handoff and relocation are presented in Section II. The discrete-event simulation model and the comparative simulation results are presented in Section III. Finally, Section IV presents the conclusions.

II. Enhanced MoM Protocol

This section provides a description of the proposed Mobile Multicast protocol. Specifically, two enhanced DMSP schemes are proposed to minimize the packet loss that occurs in basic MoM protocol during DMSP handoff and relocation.

In the first scheme, each FA tries to select two (primary and backup) DMSPs whenever the number of visiting MHs at the FA changes. Note that if all the visiting MHs at a FA are from one home network, then only one DMSP can be selected at the FA.

Otherwise, two DMSPs are selected and they send multicast packets to the corresponding FA. If one of these DMSPs stops forwarding packets due to DMSP handoff, the FA can rely on the other for multicast packet delivery, thereby greatly reducing any packet loss for the visiting MHs. This backup DMSP scheme provides trade-off between the packet loss rate and the network traffic generated by multicast packet delivery. By using backup DMSP, the packet loss rate can be greatly reduced, but the network traffic is increased at most twice as much as the single DMSP case.

In the second scheme, the basic DMSP scheme is slightly modified in order to minimize the packet loss due to the DMSP handoff. Note that the basic DMSP scheme may result in packet loss when the MH belonging to the currently serving DMSP moves out. The old FA comes to know about the movement of the MH only after its lifetime expires, while the HA comes to know about the movement of the MH as soon as it receives a registration message from a new foreign network. As a result, the HA stops sending packets to the old FA, thinking that the MH is no longer in the previous foreign network. Therefore, within the handoff duration and the MH's lifetime, the FA will not receive any packets for that group; hence, there could be packet loss. In the second scheme, the responsibility of the DMSP is extended. Specifically, when the DMSP notices that its last MH moves out by receiving a registration message from a new foreign network, it does not stop sending multicast packets to the old FA. Since the old FA is checking visiting MH's lifetime at every registration timeout (TO) interval, the old FA comes to know about the movement of the MH after its lifetime expires. Then, the old FA immediately selects a new DMSP, and also informs the previous DMSP of the DMSP_change_event. After receiving the DMSP_change_event from the old FA, the previous DMSP stops sending multicast packets to the old FA. This is the extended DMSP scheme. Since the newly selected DMSP was receiving the multicast packets from the multicast source, it can simply forward these packets to the corresponding FA with minimal added delay. Thus, the packet loss rate for the extended DMSP scheme becomes almost zero. Moreover, the network traffic for the extended DMSP scheme is relatively low. It is a little bit higher than the network traffic of the original DMSP scheme, because the extended DMSP operation requires the DMSP to con-

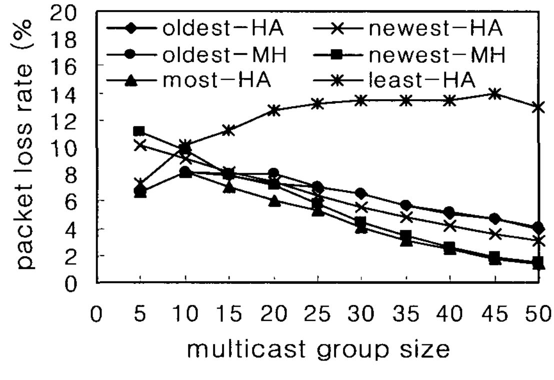
〈Table 1〉 Network and Workload Parameters

Parameter	Description	Value
N	Number of LANs	5
H	Host per LAN	10
TO	Registration timeout value (in time units)	30, 60, 90
M	Number of multicast groups	1
g	Multicast group size	5···50
λ	Multicast message generation rate (msgs/time unit)	0.1

tinue forwarding multicast packets until its last MH's lifetime has expired.

III. Performance Evaluation

This section provides performance evaluations of the proposed DMSP schemes. For performance comparisons relative to the previous approaches, the same network model in MoM protocol [2] was used. It is assumed that there are N local area networks (LANs), each with H mobile hosts. Each LAN has an associated HA and FA. In the simulation model, MHs can be in one of two states: at the home network or at a foreign network. Foreign networks to visit are chosen equiprobably at random, while the homing probability after each visit to a foreign network is 0.5. The residency time for each visit to a network (home or foreign) is drawn from an exponential distribution with a mean of 60 time units, and the travel time for going between networks (regardless of distance) is exponentially distributed with a mean of 15 time units. The network topology between the LANs is not explicitly modeled in this simulation. Thus, MHs spend 20% of their time in transit, and 80% of their time connected to a LAN (53.3% at foreign networks, and 26.7% at home network). It is assumed that there are M multicast groups. For each multicast group, group members are chosen equiprobably at random and there is a single multicast source. Also, it is assumed that each MH has a static membership of multicast groups during a simulation. Multicast messages are generated in a Poisson fashion with message arrival rate λ. Table 1 summarizes the main network and workload parameters used in the simulation experiments. In the simulation, the multicast group size was varied from 5 to 50.



〈Fig 3〉 Packet loss rates of different DMSP selection policies (TO = 60).

To evaluate the performance of the proposed multicast schemes, series of simulations have been conducted by using a discrete-event simulation package AweSim v2.0 (Pritsker Corporation). The warming-up period used for the simulations was 600 time units, following which the simulation statistics relating to mobile multicast was collected until the end of the simulation time (60000 additional time units). Simulation runs were performed on 10 different randomly generated network topologies for each set of workload parameters, with the results averaged for the purposes of plotting.

The first simulation experiment was conducted to study the degree of packet losses due to DMSP handoff, varying the multicast group size and the DMSP selection policies. Figure 3 shows the packet loss rates of different DMSP selection policies in MoM protocol with single DMSP. The packet loss rate is defined as the ratio of the number of packets lost due to DMSP handoff to the number of packets that is to be delivered to the multicast group members. Since a DMSP is to act as the forwarder for a multicast group G at a given foreign network, the number of DMSP handoff events and the packet loss rates are dependent on the DMSP selection policies. Several different DMSP selection policies were implemented in the simulation:

- Oldest-HA: The HA entry that has been in the HA list the longest time is chosen as the DMSP.
- Newest-HA: The HA entry that has been in the HA list the shortest time is chosen as the DMSP.
- Oldest-MH: The HA of the MH that has been visiting the FA the longest time is chosen as the DMSP.
- Newest-MH: The HA of the MH that has been visiting the FA the shortest time is chosen as the DMSP.
- Most-HA: The HA entry that presently has the most visitors at the FA is chosen as the DMSP.
- Least-HA: The HA entry that presently has the least visitors at the FA is chosen as the DMSP.

In the paper [2], it was shown that the oldest-HA policy performs best in terms of the number of DMSP handoff, since it always postpones handoff decisions as long as possible. However, Fig. 3 shows that the most-HA policy performs best in terms of the packet loss rate. This is because the packet loss probability can be minimized by choosing the HA having the most visitors at the FA as the DMSP. Among the DMSP selection policies, the least-HA policy performs worst, since it forces many unnecessary handoffs. In Fig. 3, it is shown that the packet loss rate of single DMSP scheme is too high for all DMSP selection policies. Therefore, enhanced DMSP schemes were proposed in this paper to reduce the packet loss rate.

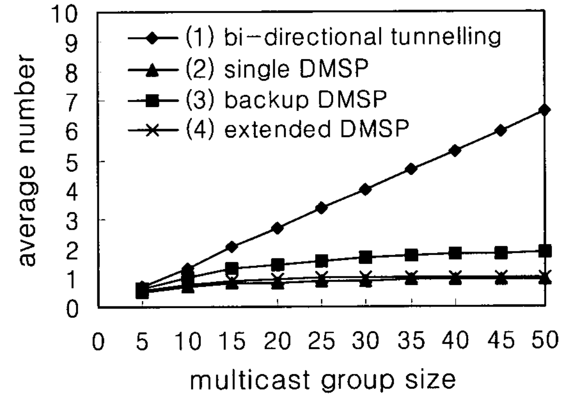
The second simulation experiment compares the performance of the proposed enhanced DMSP schemes to the previous approaches in terms of the network traffic generated by multicast packet delivery. Figure 4 shows how various aspects of the mobile routing environment scale as the multicast group size is increased. The four lines in Fig. 4 are: (1) the average number of a HA's mobile hosts that are multicast group members who are away from the home network; (2) the average number of foreign networks for which the HA is the DMSP for the single DMSP scheme; (3) the average number of foreign networks for which the HA is the DMSP for the back-up DMSP scheme; and (4) the average number of foreign networks for which the HA is the DMSP for the extended DMSP scheme.

Bi-directional tunneling requires that each HA forwards all multicast packets from groups to which its MHs are subscribed, to each MH individually. The number of packets transmitted in this approach corresponds to the average number of MHs away from home (line 1). DMSP forwarding (lines 2-4) improves upon this by restricting the number of forwarding HAs for each foreign network to some small constant number. MoM protocol with single DMSP (line 2) shows the best performance results in terms of the network traffic generated by multicast packet delivery. Note that the average number of FAs for which a HA has DMSP responsibilities is less than 1. This is because each FA assigns only one DMSP. For the backup DMSP scheme (line 3), the average number of FAs for which a HA has DMSP responsibilities is increased approximately twice as much as the single DMSP case. This is because each FA assigns two DMSPs, if available, and both DMSPs transmit multicast packets redundantly. However, by using this backup DMSP scheme, the packet loss rate can be greatly reduced as shown in Fig. 5. Thus, the backup DMSP scheme provides trade-off between the packet loss rate and the network traffic. For the extended DMSP scheme, the average number of FAs for which a HA has the DMSP responsibilities is a little bit higher than that of the single DMSP case (line 4). This is because the extended DMSP operation requires the DMSP to continue forwarding multicast packets until it's last MH's lifetime has expired. However, by using the extended DMSP scheme, the packet loss rate becomes almost zero.

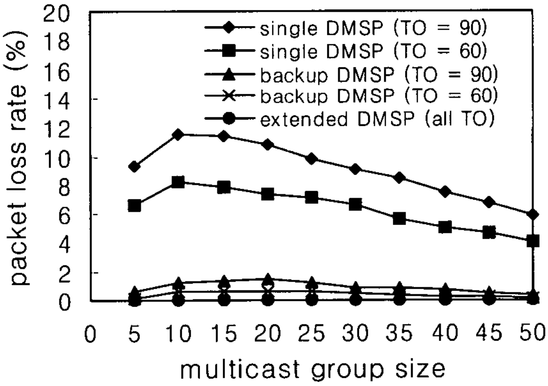
The third simulation experiment was conducted to study the degree of packet losses due to DMSP handoff, varying the timeout value and the multicast group size. Figure 5 shows the packet loss rates of three different DMSP schemes with various timeout values.

From the simulation results, it is shown that the packet loss rate increases as the timeout value at the FA increases for both single and backup DMSP schemes. This is because the larger the timeout value, it takes more time for the FA to recognize the departure of the visiting MH and perform DMSP handoff in the case that the moving host's HA was the DMSP. Until this handoff completes, multicast packet delivery for group members at the foreign network may be disrupted. By using small timeout value at the FA, the packet loss rate can be reduced. However, the processing overhead to check the existence of a MH at every timeout interval increases. Thus, there is a trade-off between the packet loss rate and the processing overhead at the FA.

For the single DMSP scheme operating at



〈Fig 4〉 Scaling characteristics of different DMSP schemes (TO = 60).



〈Fig 5〉 Packet loss rates of different DMSP schemes.

the timeout value of 60 time units and multicast group size of 25, the packet loss rate is about 7.1%. For the backup DMSP scheme operating at the same parameters, the packet loss rate is reduced to 0.59%. In Fig. 5, it is shown that the packet loss rates of the backup DMSP scheme operating at the timeout value of 60 time units are under 0.67% for all group sizes. By using the backup DMSP scheme, the packet loss rate can be greatly reduced at the expense of the increased network traffic as shown in Fig. 4.

Finally, the extended DMSP scheme has no packet loss that occurs due to the DMSP handoff, and it shows almost the same network traffic as the single DMSP scheme. The only overhead of the extended DMSP scheme is that it requires the DMSP to continue forwarding multicast packets until its last MH's lifetime has expired.

VI. Conclusions

In this paper, the packet loss problem that occurs in the MoM protocol due to DMSP handoff was investigated through simulation experiments. It was shown that the packet loss rate of the single DMSP scheme is too high for all DMSP selection policies. Therefore, two enhanced DMSP schemes were proposed to reduce the packet loss rate. The first scheme uses a backup DMSP and greatly reduces the packet loss rate at the expense of the increased network traffic. The second scheme utilizes the extended DMSP operation and shows many desirable features such as the almost-zero packet loss rate and relatively low network traffic.

References

[1] C. Perkins, “IP Mobility Support,” RFC 2002, Oct. 1996.

[2] T. G. Harrison, et al, “Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts,” *Proc. of ACM/IEEE MOBICOM’97*, pp. 151-160, Sept. 1997.

[3] C. Lin and K. Wang, “Mobile multicast support in IP networks,” *Proc. of IEEE INFOCOM’2000*, pp. 1664-1672, March 2000.

[4] C. Lin and K. Wang, “Scalable multicast protocol in IP-based mobile networks,” *ACM/Baltzer Wireless Networks*, vol. 8, no. 1, pp. 27-36, Jan. 2002.

[5] Y. Suh, H. Shin, and D. Kwon, “An efficient multicast routing protocol in wireless mobile networks,” *ACM Wireless Networks*, vol. 7, no. 5, pp. 443-453, Sept. 2001.

[6] S. Yang and S. Park, “An efficient multicast routing scheme for mobile hosts in Ipv6-based networks,” *J. Institute of Elec. Eng. Korea*, vol. 38, no. 8, pp. 11-18, Aug. 2001.

[7] S. Yang and S. Park, “An efficient mobile multicast routing for QoS guarantee in Ipv6-based networks,” *World Wireless Congress (WWC 2002)*, May 28-31, 2002.

[8] J. Park, “Mobile multicast routing protocol: TBMoM (Timer-Based Mobile Multicast),” *RMT Wksp. 2002*, May 2002.

[9] R. Boivie, Y. Imai, W. Livens, D. Ooms, and O. Paridaens, "Explicit Multicast Basic Specification," draft-ooms-xcast-basic-spec-04.txt, Jan. 2003.

◐ 저자소개 ◑

남 세 현 (Seahyeon Nam)
1985년 연세대학교 전자공학과 졸업(학사)
1987년 한국과학기술원 전기및전자공학과 졸업(석사)
1991년 한국과학기술원 전기및전자공학과 졸업(박사)
1994년 ~ 현재 대구대학교 정보통신공학부 교수
관심분야 : 컴퓨터네트워크, 광통신망, 멀티캐스트 프로토콜
E-mail : shnam@daegu.ac.kr