

정책기반 이동 IP 네트워크의 프레임워크와 정책 시나리오*

강 승 완, 김 태 경, 이 정 환, 유 상 조
인하대학교 정보통신대학원 멀티미디어통신망 연구실
전화 : 032-872-8353

A Framework and Policy Scenarios of Policy-based Mobile IP Networks

Seung Wan Kang, Tae Kyung Kim, Jung Hwan Lee, Sang-Jo Yoo
Multimedia Network Laboratory

The Graduate School of Information technology and Telecommunication Inha University
E-mail : {c2021001, c2021010, c2031019}inhavision.inha.ac.kr, sjyoo@inha.ac.kr

Abstract

Because of increasing the notebook computer and PDA, users' requirement with respect to mobility is growing more and more. However, current IP protocol is not changed IP address and can not deliver IP packets on new location of host in case moving another network. To solve this problem, the IETF has proposed mobile IP. The network management for maintaining stable and efficient environment is more difficult according to being various by complicated network environment and requirements of provided service and user. The recent rises concern about policy-based network technology. Therefore, this paper proposed a framework of policy-based network and developed policy scenarios using the presented policy language of mobile IP.

I. 서론

최근의 네트워크는 네트워크의 복잡화, 응용서비스의 다양화, 서비스 품질 제공 요구 등의 증가로 인해 네트워크의 효율적 설계, 구축, 관리, 진화에 있어 해결 해야 할 많은 문제들을 안고 있다. 정책기반 네트워크 (policy-based network)는 이러한 문제를 해결하기 위하여 최근에 도입된 네트워크 구조이다. 그리하여 정책기반 네트워크는 통신망을 관리하는 측면에서 이용자와 통신 사업자에게 편리한 시스템이다.

인터넷 사용자들은 언제 어디서나 고품질의 인터넷 서비스를 사용하기를 바라고 있으며, 휴대용 컴퓨터나 PDA와 같은 이동 단말들의 성능 향상과 무선 통신 기술 발전으로 인하여 그 사용자 수가 크게 증가하고 있으므로 무선 또는 이

동 단말을 위한 이동성 지원 기능을 포함하는 방향으로 나아갈 것이다. 그래서 IETF에서는 호스트가 이동을 하여도 IP 주소의 변화 없이 사용할 수 있는 이동 IP (Mobile IP)를 표준으로 제안하였다. 따라서 유선뿐만 아니라 이동 IP에서도 네트워크를 통한 서비스 별 자원관리 및 구성을 통합적으로 제어할 관리가 필요하다.

본 논문은 이동 IP에서도 네트워크 운용자에 따라 자동화된 정책의 수립, 전달, 실행을 지원할 수 있도록 정책기반 이동 IP 네트워크에 대한 프레임워크와 정책 클래스에 대한 각각의 정책 시나리오들을 제시한다.

II. 정책기반 이동 IP 네트워크의 프레임워크

그림 1은 정책기반 이동 IP 네트워크의 기본 구성도와 이동노드 (mobile node)가 외부 네트워크 (foreign network)로 이동하였을 때의 동작 절차를 표현하였다. 이 그림에서 정책서버는 사용자 프로파일 (사용자 ID, IP 주소 등)을 받아 그 프로파일을 바탕으로 사용자에게 알맞은 정책을 결정하고 구성하며 장비에 그 정책을 전송하여 사용자에게 최적의 서비스를 제공하려는데 목적이 있다.

다음은 이동 단말이 외부 네트워크로 이동하였을 때 정책기반 이동 IP 네트워크의 동작 절차를 설명한다(외부 에이전트 care of address를 이용하였을 때의 동작 절차를 가정한다).

- (1) 가입자가 외부 네트워크에 접속하였을 때, 가입자는 외부 에이전트 (foreign agent)에게 등록 요청과 더불어 사용자 ID와 인증에 필요한 정보를 보낸다.
- (2) 외부 에이전트는 이 정보를 AAA 서버에 전달하고 AAA 서버는 Network Access Identifier (NAI)와 비교하여 이 정보를 분석한다. 동시에 외부 에이전트는 등록 요청 정보를 이동 단말의 인증이 허락될 때까지 등록 요청 정보를 유지한다.

* 본 연구는 한국한술진흥재단 선도연구자지원 (D00378)으로 수행되었음

- (3) AAA 서버는 외부 네트워크 뿐만 아니라 홈 네트워크도 인증을 관리하고 있다. AAA 서버는 인증 절차를 수행한 후 인증에 성공하면 가입자의 접속을 허락하고 가입자 인증 허락 메시지를 외부 에이전트에 보내는 동시에 정책서버에게 가입자가 로그인 되었다는 이벤트를 보낸다.
- (4) 외부 에이전트는 가입자의 원래 속해있던 홈 네트워크의 홈 에이전트(home agent)에 등록 요청을 함과 동시에 정책서버는 LDAP 프로토콜을 이용하여 정책저장소(policy repository)에 해당 가입자 정보를 요청한다.
- (5) 홈 에이전트가 등록 요청을 허락하면 등록 응답 메시지를 외부 에이전트에게 보내고 정책 저장소는 현재 기록되어 있는 가입자 정보에 대한 정책 정보를 LDAP 프로토콜을 이용하여 정책서버에 보낸다.
- (6) 정책 서버는 정책 저장소에서 보내는 정책 정보를 바탕으로 실행할 정책을 결정하고 결정된 정책은 COPS 프로토콜을 이용하여 장비에게 전달하며, 장비들은 정책을 수행할 수 있도록 셋업(setup)이 되고 요구된 서비스가 이용할 수 있음을 사용자에게 통보한다.
- (8) 그 후, 가입자는 정책에 따라 서비스를 제공받는다.

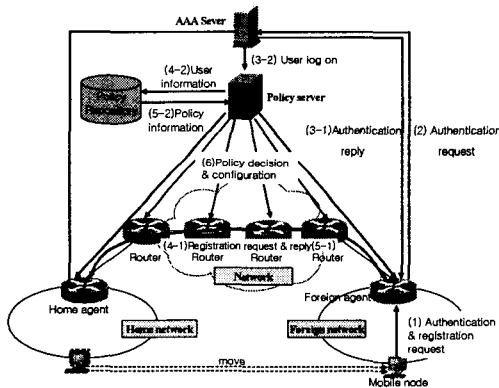


그림 1 정책기반 이동 IP 네트워크 구성도와 동작절차

정책기반 이동 IP 네트워크 구조는 그림 2와 같다. 정책서버는 크게 응용 계층(application layer), 제어 계층(control layer), 결정 계층(decision layer) 3가지로 나눌 수 있다. 세부적으로 들어가면 정책을 지시하고 변경하고 디스플레이 하는 사용자 인터페이스를 제공하는 정책 관리 도구(policy management tool), 네트워크 접근을 관리하는 접근 관리자(Access Manager), 서비스 품질을 관리하는 QoS 관리자(QoS Manager), 이동 IP에 관련된 관리를 하는 이동 IP 관리자(Mobile IP Manager), 장비들을 모니터를 하는 모니터링 관리자(Monitoring Manager), 정책 규칙과 관리되고 있는 서비스 및 네트워크 장치의 상태로 기초로 필요한 정책을 결정하는 정책 결정 점(policy Decision Point, PDP)으로 구분된다. 정책 정보를 저장하고 입/출력하는 저장 장치인 정책 저장소(Policy Repository)와 사용자의 인증, 권한, 과금을 관리하는 AAA 서버는 정책서버와 연결이 되었다. 정책 저장소와 PDP는 LDAP 프로토콜로 연결이 되며, AAA 서버와 PDP는 DIAMETER 프로토콜로 그리고 정책서버와 이동 에이전트는 COPS 프로토콜로 연결이 되어있다. 장비 계

층(device layer)은 여기에서 이동 에이전트이고, 이동 에이전트는 홈 에이전트와 외부 에이전트를 가리키는 것이다. 에이전트는 크게 관리층(management plane)과 전달층(forwarding plane)으로 구분이 된다. 관리층은 네트워크 접근을 제어하는 접근 제어(access control), 에이전트에서 QoS 제어하기 위한 QoS 제어(QoS control), 이동 IP 동작을 제어하는 이동 IP 동작 제어(Mobile IP Operation control), 이동 노드가 이동중에도 끊김이 안되도록 해주는 핸드오프 제어(handoff control)가 있다. 전달층은 패킷을 전송해주는 전달 경로(forwarding path) 계층이다.

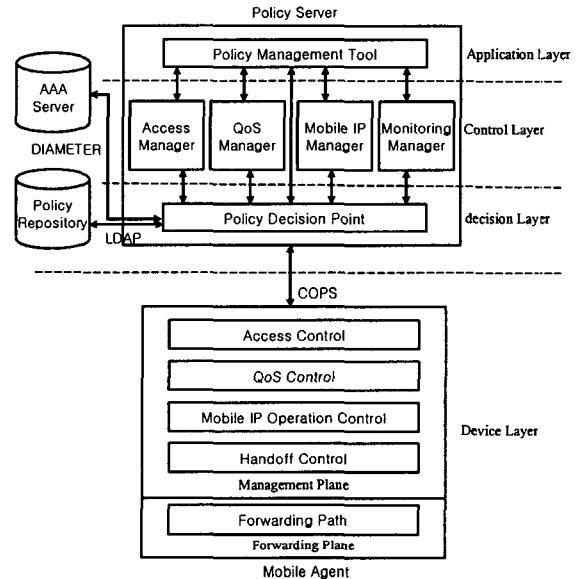


그림 2 정책서버와 이동 에이전트 구조

III. 정책기반 이동 IP네트워크의 정책 시나리오

본 논문에서는 정책기반 이동 IP네트워크의 정책들을 클래스 별로 나누었다.

그림 3은 정책 클래스를 추상적으로 표현한 것이다.

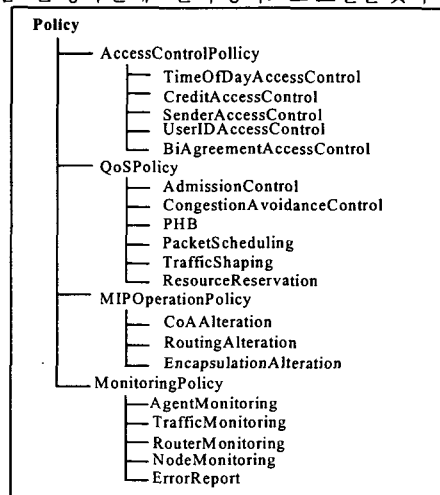


그림 3 정책 클래스

정책 클래스는 크게 가입자의 접근을 허락하거나 불허하는 접근 제어 정책 (AccessControlPolicy), 가입자에게 서비스 품질을 할당하는 정책 (QoSPolicy), 이동 IP의 동작을 제어하는 정책 (MIPOperationPolicy)과 모니터링 정책 (MonitoryPolicy)으로 구분한다.

접근 제어 정책은 가입자의 형태, 가입조건에 따른 시간대에 접근을 허용하거나 불허하는 시간에 따른 접근제어 정책 (TimeOfDayAccessControlPolicy), 가입자의 신용도(과금 결제 내역등)에 따른 신용도에 의한 접근제어 정책 (CreditAccessControlPolicy), 송신자가 해당 트래픽을 수신할 수 있는 수신자를 지정해줄 수 있는 송신자 접근제어 정책 (SenderAccessControlPolicy), 사용자 ID를 기초로 접근을 허락하거나 불허하는 사용자 ID 접근제어 정책 (UserIPAccessControlPolicy), 양방향 계약 접근제어 (BiagreemntAccessControl)들로 나눌 수 있다. 서비스 품질 정책은 가입자 트래픽이 네트워크를 통과할 때 대역폭을 할당을 해주는 수락제어 정책 (AdmissionControlPolicy), 전송률의 지연 또는 패킷이 버려짐에 의한 혼잡을 제어해주는 혼잡 회피 정책 (CongestionAvoidance), 트래픽을 미리 예약할 수 있는 자원예약 정책 (ResourceReservationPolicy), 그리고 DiffServ 서비스를 제공하기 위해 들어온 패킷을 코드 포인트 (DSCP) 값으로 PHB (per-hop behavior)를 할당하는 PHB 정책 (PHBPolicy), 서비스 요구에 따라 클래스들을 만족시킬수 있는 패킷 스케줄링 정책 (PacketSchedulingPolicy), 트래픽의 속도를 제어하는 트래픽 셰이핑 정책 (TrafficShapingPolicy)으로 나눌 수 있다. 이동 IP 동작을 제어하는 정책들은 care of address를 변경시켜주는 care of address 변경 정책 (CoAAlterationPolicy), 이동 IP의 라우팅을 변경시키는 라우팅 변경 정책 (RoutingAlterationPolicy), 캡슐화를 변경시켜주는 캡슐화 변경 정책 (EncapsulationAlterationPolicy)으로 나뉜다. 모니터링 정책은 홈과 외부에이전트를 모니터링하는 에이전트 모니터링 정책 (AgentMonitoryPolicy), 트래픽을 모니터링

는 트래픽 모니터링 정책 (TrafficmonitoryPolcicy), 라우터를 모니터링하는 라우터 모니터링 정책 (RouterMonitoryPolicy), 단말을 모니터링하는 단말 모니터 정책 (NodeMonitorypolicy), 이 네트워크의 에러를 검사하여 에러가 나타난 곳을 보고하는 에러 리포팅 정책 (ErrorReportPolicy)을 나타낸다.

본 논문은 이들 정책 클래스를 가지고 정책 시나리오를 나타내기 위해 이 논문에서 제안한 정책 언어로 정책을 표현하였다. 그림 4-1은 정책 선택의 (syntax)로서 이 선택을 바탕으로 클래스들의 정책들을 표현하였다. Title은 표현할 정책의 제목을 표시하는 곳이다. Subject는 정책을 지시하는 주체 즉, 관리자나 정책 서버를 가리킨다. Initiator는 맨 처음 정책을 지시하는 주체에게 정책을 청원하는 위치를 가리키고, Target은 주체에서 명한 정책을 실질적으로 실행하는 곳을 가리킨다. On은 event-trigger 즉, 어떠한 상황에서 이 정책이 발생하는 지를 나타내고, Policy에서 If는 정책의 조건(condition)을 나타내고 Then은 조건이 결정된 후 그것을 실행하는 행동 (action)을 표현한다. 그림 4-2부터 4-6은 각각 클래스에 대한 정책들의 예이다.

● 시간에 따른 접근 제어 정책

시간에 따른 접근 제어는 관리자가 가입자의 형태, 가입 조건에 따라 하루 중 또는 년 중 특정시간대에 네트워크 접근을 허용하거나 혹은 불허하는 정책이다. 이 정책의 예를 그림 4-2로 표현하였다. 즉, 가입자가 주중의 비즈니스 시간대(9시~17시)에만 네트워크 접근을 허용하는 예이다. 이동 노드가 홈 에이전트나 또는 외부 에이전트에 접근을 하면 홈 에이전트나 외부 에이전트는 정책서버에게 질의를 한다. 정책 서버의 접근 관리자 (access manager)는 가입자의 정보를 확인하여 먼저 비즈니스 시간에 접속하였는지를 알아본 후 정책을 할당한다. 이동 노드가 주중의 비즈니스 시간대에 접근을 하면 정책 서버는 이동 단말의 접근을 허락하고 그 시간대가 아니면 접근을 불허하는 정책을 표현하였다.

| | | |
|---|---|--|
| <p>Title policy name;</p> <p>Subject indicates policy ;</p> <p>Initiator firstly invokes policy;</p> <p>Target executes policy;</p> <p>On event-trigger;</p> <p>Policy If Condition Then Action;</p> <p>4-1. 정책 선택</p> | <p>Title TimeOfDayAccessControlPolicy;</p> <p>Subject AccessManager;</p> <p>Initiator HA FA;</p> <p>Target //HA is a home agent and FA is a foreign agent HA FA;</p> <p>On MNAccessRequest; //MN is a mobile node</p> <p>Policy If DayOfWeek == MonToFri && TimeOfDay == 0900To1700; Then MNAccessAdmission;</p> <p>4-2. 시간에 따른 접근 제어 정책의 예</p> | <p>Title BiAgreementAccessControlPolicy;</p> <p>Subject AccessManager;</p> <p>Initiator FA;</p> <p>Target HA && FA;</p> <p>On MNAccessRequest && HomeNetworkOfMN ≠ SameDimension;</p> <p>Policy If (HA && FA) == BiAgreement; Then MNAccessAdmission;</p> <p>4-3. 양방향 계약 접근 제어 정책의 예</p> |
| <p>Title ResourceReservationPolicy;</p> <p>Subject QoSManager;</p> <p>Initiator PolicyServer;</p> <p>Target FA && Router;</p> <p>On MNAccessAdmission;</p> <p>Policy If MNProfile == ResourceReservation; Then FA && Router ::= ReservedResource;</p> <p>4-4 자원예약 정책의 예</p> | <p>Title RotingAlterationPolicy;</p> <p>Subject MibileIPManager;</p> <p>Initiator HA;</p> <p>Target CN && HA && FA;</p> <p>On // CN is a correspondent node CNTToFA ∈ SameDomain;</p> <p>Policy If Routing == TriangleRouting; Then Routing ::= RouteOptimization;</p> <p>4-5 라우팅 변경 정책</p> | <p>Title EncapsulationAlteratinPolicy;</p> <p>Subject PolicyServer;</p> <p>Initiator HA;</p> <p>Target HAToFA;</p> <p>On Network = = Congestion;</p> <p>Policy If FASupportsMinimalEncapsulation; Then HA ::= MinalEncapsulation;</p> <p>4-6 캡슐화 변경 정책의 예</p> |

그림 4 정책 시나리오

- **양방향 계약 접근 정책**
 홈 에이전트와 외부 에이전트의 동의 하에 이동 노드의 접근을 허락하는 정책이다. 그림 4-3은 이 정책의 예를 표현한 것으로서 어떤 하나의 이동노드가 외부 에이전트에 접근을 하였을 때, 이동노드의 홈 에이전트가 타 가입자망의 네트워크에 속하면, 정책서버의 접근관리자 (Access Manager)는 그 가입자망의 계약을 맺고 있는지를 확인하여 그 가입자망과 계약이 맺어 있으면, 타 가입자망에 속한 홈 에이전트와 외부 에이전트가 등록하여 이동 노드가 서비스 받을 수 있도록 해주는 정책의 예이다.
- **자원 예약 정책**
 가입자가 미리 예약한 자원으로 서비스를 받는 정책으로, 그림 4-4는 이러한 정책의 예를 표현하였다. 이동노드의 접근이 허락한 후에 정책서버는 외부 에이전트에 접속한 가입자 프로파일을 확인하여, 그 프로파일에 자원 예약이 명시되어 있다면 외부 에이전트와 라우터에서 그 명시된 자원 예약을 실행시키는 정책을 표현한 것이다.
- **라우팅 변경 정책**
 라우팅 변경은 네트워크 상황에 따라 삼각 라우팅 (triangle routing)에서 경로 최적화 (route optimization)으로 또는 경로 최적화에서 삼각 라우팅으로 정책을 줄 수 있다. 그림 4-5가 이러한 정책의 예를 보여준다. 이 정책은 외부 에이전트 care of address를 사용한다는 가정 하에 상대 노드 (correspondent node)에서 외부 에이전트까지 같은 도메인 A에서 삼각 라우팅으로 패킷을 송수신하고 있다면, 지연 증가와 성능 저하가 나타난다. 그래서 상대 노드와 외부 에이전트까지 같은 도메인 A에서 패킷을 송수신하는 것은 경로 최적화로 패킷을 송수신하게 정책을 주도하도록 표현하였다.
- **캡슐화 변경 정책**
 터널링을 위해 패킷은 캡슐화를 하는데 이 캡슐화 기법으로는 일반적으로 IP-in-IP 캡슐화 방법을 사용한다. 그러나 홈 에이전트와 외부 에이전트 사이에 네트워크 혼잡이 발생하면 IP-in-IP 캡슐화한 패킷은 패킷 지연이 발생한다. 그러므로 이 패킷 지연을 우려하여 패킷 크기를 최소로 캡슐화하는 최소 캡슐화 (minimal encapsulation)로 변경한다. 그림 4-6의 정책은 IP-in-IP 캡슐화 기법에서 최소 캡슐화 기법으로 변경하는 정책의 예이다. 외부 에이전트는 정책서버에게 정책을 문의하고, 정책서버의 이동 IP 관리자는 홈 에이전트에서 외부 에이전트로 네트워크 혼잡이 발생한다고 판단되고, 외부 에이전트가 최소화 캡슐화를 지원한다면, 캡슐화를 담당하는 홈 에이전트에게 최소화 캡슐화로 변경한다는 정책을 전달하고 홈 에이전트가 그 정책을 실행한다.

문에서 제한하는 정책 언어를 사용하여 제시하였다.

향후 과제로는 본 논문을 기초로 이동 IP DiffServ환경에서의 정책 프레임워크, 정책 스키마, 정책 시나리오들과 무선망에서의 QoS를 제공하는 정책기반 네트워크를 연구한다. 그리고 이 연구들을 기반으로 테스트베드를 구축하여 정책기반 이동 IP 네트워크를 구현하여 볼 것이다.

참고 문헌

- [1] C. Perkins, "IP Mobility Support for IPv4", RFC 3220, IETF, 2002
- [2] Dave Kosiur, "Understanding Policy-Based Networking", John Wiley & Sons, Inc. 2001
- [3] James D. Solomon, "Mobile IP: The Internet Unplugged", Prentice Hall, Inc. 1998
- [4] Leonidas Lymberopoulos, Emil Lupu and Morris Solman, "An Adaptive Policy Based Management Framework for Differentiated Services Networks", Proceedings of the Third International Workshop on Policies for Distributed System and Network (POLICY'02), pp. 147-158
- [5] Paris Flegkas, Panos Trimintzios, and George Pavlou, "A Policy-Based Quality of Service Management System for IP DiffServ Networks", IEEE Network, Volume 16, Issue 2, pp. 50-56 March/April 2002,
- [6] Wang Changkun, "Policy-based Network Management", International Conference on Communication Technology Proceedings Volume 1, pp. 101-105, 2000
- [7] Zheng Wang, "Internet QoS: Architectures and Mechanisms for Quality of Service", Morgan Kaufmann Publishers, Inc. 2001
- [8] Yuji Nomrua, Akira Chugo, Motomitsu Adachi and Masahito Toriumi "A Policy Based Networking Architecture for Enterprise Networks", IEEE International Conference on Communications (ICC'99), Volume 1, pp. 636-540, 1999
- [9] White Paper, "A Primer on Policy-based Network Management" Hewlett-Packard Company, September 24, 1999

IV. 결론 및 향후과제

본 논문은 정책기반 이동 IP네트워크의 프레임워크, 동작 절차, 정책 서버와 이동 에이전트의 구조를 표현하였다. 그리고 정책기반 이동 IP 네트워크의 정책들을 클래스 별로 나타내었고, 클래스에 따른 각각의 정책 시나리오는 본 논