정책기반 네트워크 관리 구조의 분석과 평가

임 형 진[†] · 이 현 주[††] · 이 종 혁[†††] · 정 태 명[††††]

요 약

본 논문에서는 정책 기반 네트워크 관리에 대한 중앙 집중 형태와 분산 형태의 모델을 비교하고 모델링하기 위한 분석적인 프레임워크를 제안했다. 정책기반 네트워크는 다양한 응용분야에서 도입되고 있으며, 정책의 제공구조는 응용에 따라 각기 다른 처리성능을 가질 수 있다. 따라서 우리는 각 PBNM 모델이 정책 적용을 수행할 때 성능과 확장성 측면에서 평가하였다. 측정 메트릭으로는 정책 프로비저닝 시간, 트래픽 발생량, PDP 처리율, 전역 충돌 감지에 대한 정성적 시뮬레이션을 평가하였다. 그 결과 PBNM을 도입할 때 주의 깊은 응용 특성에 대한 분석에 따라 적절한 구조가 도입되어야 함을 제시하고 있다. 본 논문에서 나타난 PBNM 모델은 현재 제안되고 있는 방식들 사이에 장단점을 정량화하기 위한 시도였다.

An Analysis and Evaluation of Policy-Based Network Management Approaches

Hyung J. Lim[†] · Hyun J. Lee[††] · Jong H. Lee[†††] · Tai M. Chung[††††]

ABSTRACT

This paper proposed an analytical framework to compare and model the policy-based network management; centralized and distributed typed model. Policy-based network is introduced in various application fields, and a policy framework can offer different processing performance according to application. Therefore, we evaluated the performance and extensibility of each PBNM model when we apply the policy process to the models. The evaluated measurement metrics are policy provisioning time, traffic occurrence amount, PDP processing rate, and global conflict detection in qualitative simulation. The results show that the suitable structure is required according to the analysis for the careful application characteristics, when PBNM is adopted. The modeling framework presented in this paper is intended to quantify the merits and demerits among the currently suggested PBNM models.

키워드: 정책기반 네트워크 관리(Policy-Based Network Management(PBNM)), 네트워크 관리(Network Management), 네트워크 제어(Network Control)

1. 서 론

현재 대부분의 Simple Network Management Protocol (SNMP)나 Common Management Information Protocol (CMIP)을 이용한 네트워크 관리 체계는 관리자에게 있어서 관리에 대한 효율성을 제공하여 줄 수 있지만, 네트워크 관리 기술의 주된 응용인 장애 감지나 수정, 복구만을 통해서는 이러한 복잡한 네트워크 환경과 다양한 사용자의 요구를 충족하기에 한계가 있다[1]. 이런 요구사항 만족을 위해서 지능형 제어 기술이 도입 되지만 근본적으로 사용자의 서비스 요구와 네트워크 상태 정보에 기반하여 적절하게 네트워크를 제어 할 수 있는 구조를 요구하고 있다[2-3]. 따라서 기존의 네트워크 관리 구조의 확장 형태로서 정책기반 네트워크 관리 구조(Policy Based Network Management; PBNM)가 제안되고 있다. PBNM은 네트워크 제어를 위한 기술로서 연구가 시작되었으며, 초기에는 QoS 분야에서 도입되었으며, 보안 분야에서도 다양하게 적용되고 있다.

정책기반 네트워크 관리는 비즈니스 및 서비스 레벨의 관리 정책을 정의하고, 이를 기반으로 네트워크 및 서비스를 자동으로 관리하는 기술이다. 관리 정책을 정의함에 있어서, IETF 및 DMTF에서 정의한 Policy Information Model (PIM)를 사용하여 관리정책을 정의하도록 권고하고 있다. 정책은 네트워크 관리 영역뿐만 아니라 응용들의 서비스 요구 수준을 제공하기 위하여 정의된다. 따라서 정책은 네트워크 디바이스에서 수락(accept), 요청(request), 강화(enforce)하는 동작을 수행하며, 네트워크 디바이스가 인식할 수 있

※ 성균관대학교 응급의료 정보시스템 개발센터
본 논문은 보건복지부 보건의료기술진흥사업회 지원에 의하여 이루어진 것임 (과제번호 : 02-PJ3-PG6-EV08-001)
† 정 회 원 : 성균관대학교 컴퓨터공학과 박사과정
†† 준 회 원 : 성균관대학교 컴퓨터공학과 석사과정
††† 준 회 원 : 성균관대학교 컴퓨터공학과 석사과정
†††† 종신회원 : 성균관대학교 정보통신공학부 정교수
논문접수 : 2004년 7월 24일, 심사완료 : 2004년 12월 30일

고, 실행 가능한 로직으로 표현되어야 한다. 전통적인 장비들에 추상적인 정책을 구현하기 위해서는 네트워크 구조에 추상 레벨 (Abstract Network Layer: ANL)로 기능을 수행하는 PDP(Policy Decision Point)와 PEP(Policy Enforcement Point)가 구현되어야 한다. 또한 정책이 적용되고 있는 네트워크 상태를 모니터링 할 구조와 네트워크의 상태변화에 따른 자동화된 정책 제공 구조가 요구된다[4-7].

전통적인 네트워크 관리 시스템에서는 프로세싱 시간, 관리 노드의 처리부하 그리고 관리 트래픽 발생량이 성능에 영향을 미치는 요소이다[1]. 그러나 제어시스템으로서 PBNM의 성능에 영향을 미치는 요소는 정책의 표현과 장치레벨로의 정책 번역뿐만 아니라 정책 충돌 해결과 분배 방식에 따른 적용 성능이 고려되어야 한다. 그러나 기존의 연구들을 살펴보면 네트워크의 복잡한 규모에 따른 확장성과 정책 적용 성능 보다는 특정 응용에 대한 정책 적용 가능성만을 고려한 PBNM 프레임워크를 설계하고 있다[9-12].

PBNM기반의 네트워크 관리 접근들은 기본적으로IETF에서 제안하는 2계층 구조로서 제안되었다[13-15]. 그러나 A Corrente[16]은 2계층 구조에서 정책 복잡도에 따른 PDP의 병목현상 문제를 제시하였다. 또한, 3계층 구조[17]이 QoS 적용을 위한 IETF표준화과정에서 언급되었고, Eddle Law [18]는 2계층에 대한 확장성 문제와 PDP에서 병목문제가 있음을 제시하며 3계층 구조를 제안하였다. 그러나 단일 도메인 안에서 PBNM을 구성하는 컴포넌트간의 정책 적용이 발생할 때 PDP의 처리성능만을 평가하였다. PBNM의 구조와 규모는 PDP의 처리성능 뿐만 아니라 개별 정책 프로비저닝 성능에 영향을 줄 수 있다. 또한 다중의 PDP가 사용되는 경우에는 보안성의 지원과 정책간의 충돌이 성능에 미치는 영향도 고려해야 한다.

본 논문에서는 정책 기반 네트워크 관리에 대한 접근 사례를 통해 대표적인 모델로서 단일 구조, 계층적 구조, 계층적 혼합 구조들을 분류하고, 각 모델에 따라 성능에 영향을 미치는 메트릭에 따라 제안 구조의 효율을 평가하고자 한다. 따라서 본 논문 2절에서는 PBNM을 동작하게 하는 매개로서 정책의 생명주기(Policy Life Cycle)와 제안 모델을 분류한다. 3절에서는 PBNM의 모델에 따라 성능에 영향을 줄 수 있는 메트릭에 대해서 평가한다. 4절에서는 각 제안 방식들의 평가 결과에 대한 분석을 제시한다.

2. 정책 기반 네트워크 관리

2.1 정책 생명 주기

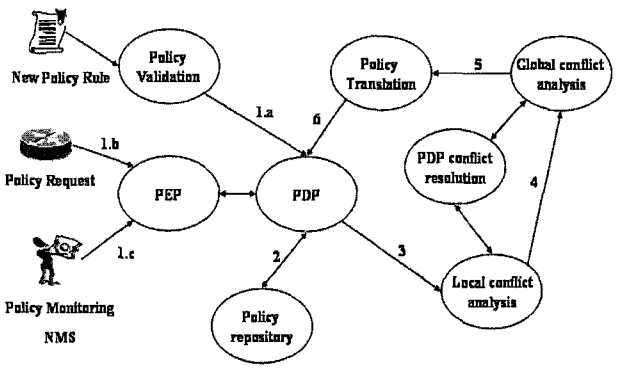
네트워크와 시스템 사용자들은 응용에 요구되는 서비스 수준을 만족하기 위해서 적절한 자원 제공을 요구한다. PBNM에서 이러한 사용자들의 응용요구는 정책으로서 표현된다. 따라서 정책은 네트워크와 시스템의 자원을 제공하기 위한 동기가 된다. 이러한 정책의 일관된 적용을 위해서는 기존의 네트워크 관리 시스템을 통해서 현재 실행되고 있는 정책에 대한 적용 상태가 모니터링 되어야 한다. 또한 정책 적용 상태 변화에 대하여 적절하게 조정될 수 있는 정책의 적응성이 요구된다.

사용자의 서비스 요구에 기반을 둔 정책은 PBNM 구성 요소들로부터 일련의 처리 절차를 통하여 자원을 할당받게 된다, (그림 1)에서는 정책의 생성으로부터 적용 때까지 생명주기를 보여주고 있다. 정책 적용은 요청의 처리 범위와 절차에 따라 Internal, Outsource, Interactive 의 방식이 사용되고 있다[7, 20, 22]. PBNM에서는 PDP로부터 정책을 동작하도록 하는 이벤트로서 정책 관리 도구(Policy Management Console)를 통하여 관리자에 의해 새로운 정책이 생성되었을 때(1.a-Internal), 시그날링 프로토콜이나 수신된 패킷의 정보들을 통하여 서비스 요청이 트리거 될 때(1.b-Outsource), 그리고 네트워크 관리시스템과 같은 PBNM 외부의 개체로부터 트랩이나 폴링을 통하여 수집된 정보를 통한 경고를 수신할 때(1.c-Interactive)로 정책 적용과 처리 방식을 구분할 수 있다.[19, 20].

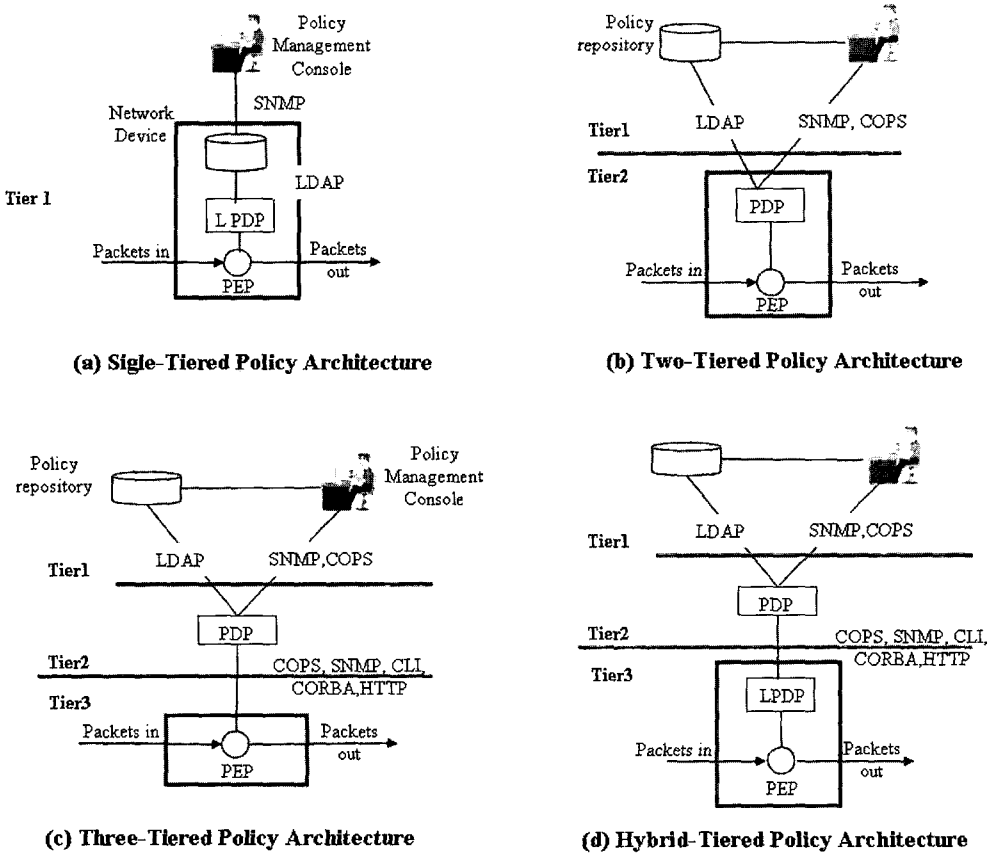
새로운 정책이 생성(1.a) 될 때는 정책 관리 도구에서 정책에 대한 무결성과 일관성을 위하여 정책 검증과 GCD (Global-policy conflict Detection) 과정을 거치게 된 후에 정책 저장소와 PDP로 저장된다. 또한, PEP 참조를 통해서 현재 디바이스의 처리 능력과 설정 정보 그리고 현재의 상태를 체크하게 된다.

다양한 소스로부터 정책 요청에 해당하는 이벤트(1.b, 1.c)를 수신한 PDP는 정책 저장소를 조회하고 정책 충돌을 검사한 후 해당 정책을 PEP에 적용할 수 있다 (그림1-(2)).

PBNM의 처리 성능문제와 서비스 제공능력 관점에서 고려되어야할 문제 중 하나는 정책 충돌(Policy conflict)과 해결(Resolution)방법이다. 정책 충돌은 서비스의 요청 과정, 정책의 정의 과정, 정책의 적용 과정에서 현재 네트워크 디바이스가 가지고 있는 처리 능력 안에서 제공 가능한 서비스 수준과 기존에 정의된 정책들 간에 논리적 위배로 발생할 수 있다. 따라서 이러한 정책충돌 해결을 통해 적절한 리소스가 할당될 수 있는 메커니즘이 제공되어야 한다. 또한 네트워크에서 적용 되었던 정책을 변경/수정할 때 지역적인 혹은 전역적인 정책 충돌 문제가 발생할 수 있으며, 이를 해결할 수 있어야 네트워크 관리 도메인 전체에 일관성 있는 정책이 적용될 수 있다[21, 22].



(그림 1) 정책 생명 주기



(그림 2) 정책 기반 네트워크 구조

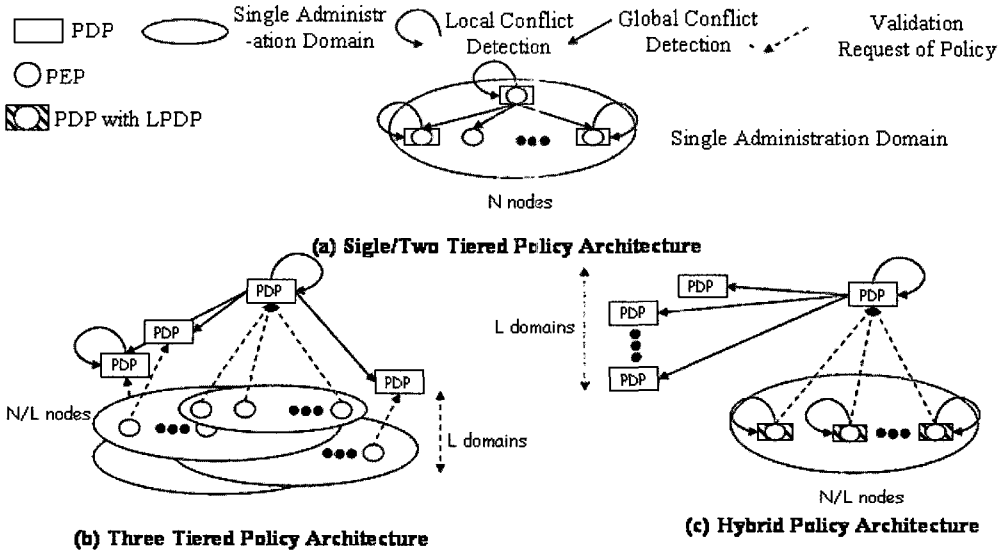
(그림 1)에서 보여주는 바와 같이, LCD(Local-Policy Conflict Detection)모듈은 특정 PDP에 연관된 디바이스나 인터페이스 레벨에서의 충돌 분석을 포함하고(그림1-(3)), GCD모듈은 PDP간의 충돌 분석(그림1-(4))을 포함한다. 정책 충돌이 발생할 경우 PDP 정책 해결모듈에서 적절한 알고리즘[23]에 따라 처리할 수 있다. 정책 충돌이 없다면 PIB (Policy Information Base) 형태로 변환된 정책은 PEP로 전송되고, 장비에 설정 가능한 벤더 의존적인 정책 명령으로 번역된다. 이때 PEP는 정상적으로 정책이 적용되었음을 PDP에 알린다. 향후 PDP와 PEP 그리고 정책저장소 간에는 상태 변화가 발생할 때 상호간의 공지(notification)를 통한 동기(synchronous)가 요구된다.

2.2 접근 모델과 가정

PBNM은 제공해야 하는 서비스와 이를 지원하는 네트워크 디바이스가 가지고 있는 제공 능력에 따라 가상의 논리적 네트워크 인프라를 구성하게 된다. (그림 2)에서는 이러한 서비스 역할을 수행하기 위한 정책기반 네트워크 구조를 나타내고 있다. PBNM 구성 요소들의 일반적인 역할을 살펴보면, PEP는 서비스 제공을 위해 정책을 디바이스 의존적인 명령어를 통해 실제 정책을 수행하는 모듈이다. NMS에서는 네트워크나 디바이스의 상태가 변화하는 이벤트가 발생할 때 PEP로 알려주어야 한다. PDP는 정책 관리 도구로부터 정책을 생성할 때나 네트워크의 상태가 변화하여 이벤트를 받을 때 정책 처리를 위해 동작한다. 또한 PDP는 정책 저장소로부터의 정책 참조, 정책의 번역, 검증 그리고 정책을 인식하지 못하는 네트워크 디바이스들에 대한 프락시로서 기능을 수행 한다.

(a)는 싱글 박스 형태로 구성되는 PBNM 구조를 나타내고 있다. 이 구조는 전통적인 네트워크장비나 시스템에서 구성되는 기본 방식이다. 이 구조의 특징은 ANL을 장비내부에 모두 수용하기 때문에 PDP와 PEP간의 통신 프로토콜이 필요 없고, 관리자에 의해 정의되는 정책이 장비 내부에 저장된다. 단일 장비에 정책이 유지되기 때문에 전체 네트워크에 대한 관리 측면에서 규모 확장성은 떨어질 수 있다[4].

(b)의 경우는 중앙 집중형 저장소와 분산형 PDP구조를 나타내고 있다. 이 구조는 개별 장비들이 PDP 모듈을 가지고 있거나, 원격의 PDP를 포함한 노드에 의해서 PDP를 수용하지 않은 노드들에 대한 정책 제공이 가능할 수 있다. PDP와 PEP가 같은 장비 내에 수용되어 있어 정책의 검증과 강화가 도메인 단위가 아닌 모든 장비에서 개별적으로 수행되거나, 원격의 PDP를 포함하는 장비에서 처리되어야 한다. 저장소 와 PDP 간에는 LDAP, SNMP, CLI 등이 사용될 수 있다[4, 15].



(그림 3) 충돌 감지 절차

(c)의 경우는 정책 저장소와 PDP가 중앙 집중 형태로 구성되지만, 장비 내부에 위치하는 PEP와는 별도로 구성된다. 이 모델은 IETF에서 제안하는 기본 프레임워크이다. 따라서 NMS로부터의 네트워크의 상태 변화나 정책 충돌에 대한 검증을 취합하여 PDP에 요청할 수 있다. 또한 정책 저장소로부터 가져온 정책을 PDP 하위 장비들에 일관성 있게 적용할 수 있다. 여러 개의 PDP가 존재할 경우 GCD를 감시하기 위하여 PDP간의 정책 분석이 요구된다. PDP와 PEP간의 통신은 CLI, SNMP, HTTP, CORBA, COPS등이 사용될 수 있다[16, 17].

(d)의 경우는 (c) 구조의 계층적인 확장 형태로서 각 디바이스에 LPDP(Local PDP)가 위치하는 구조이다. PEP는 정책에 대한 로컬 결정을 하기 위해 LPDP를 사용한다. 따라서 LPDP의 경우 PEP로부터의 서비스 요청이나 상태의 변경에 대해 빠르게 반응할 수 있는 역할을 한다. 일단 로컬 노드에서의 결정이 이루어진 후에 PDP로 원래의 요청이 전송 처리 된다. 그리고 PDP는 LPDP에서 적용되는 정책에 대하여 최종 결정권을 가지며, 그 결정 정보에 대하여 LPDP와 같은 상태 정보를 공유한다. LPDP의 경우 디바이스 내에 정책을 저장하기 때문에 유지되는 정책 수는 한계가 있을 수 있다. 따라서 현재 적용되는 정책 중심으로 구성된다[17, 18].

본 논문에서는 PDP와 PEP간 정책 전송은 COPS 프로토콜을 사용함을 가정한다. 또한, 네트워크에서는 임의의 응용이 수행되고 있고, 네트워크에서의 모든 자원은 정책을 인식하고 수행한다고 가정한다. 정책의 임시저장소의 참조에 대한 성능은 정책의 프로비저닝에는 직접적으로 영향을 미치지 않는 독립적 요소이다. 따라서 정책 저장소의 분산도에 의한 성능은 또 다른 영역으로서 고려하지 않았다. PDP는 일반적으로 정책서버 형태로서 구현됨에 따라 정책 저장소에 저장된 정책의 대부분을 보유하고 있다. PDP와 PEP에는 PIB라고 하는 정책변환과정에서의 임시저장소를 공유하고 있고, PDP의 PIB에는 PEP에 적용되어진 i개의 정책을 유지하고 있다. 따라서 PEP에는 i개의 명령이 설정되어 있기 때문에 PDP와 PEP는 i개의 정책을 공유하고 있다. 새로운 정책을 생성하는 경우를 제외하고는 외부의 이벤트에 의한 정책은 PEP와 PDP에서 보유하고 있는 것으로 가정한다. 만약 정책이 존재하지 않을 경우 관리자나 혹은 자동적인 방법에 의해서 정책을 생성해야한다. 마찬가지로, GCD가 발생할 경우 새로운 정책을 생성하거나 정책에 대한 해결 알고리즘에 따라 정책 충돌을 해결해야 한다.

일반적으로 성능에 대한 인자는 특정임무를 완료하는데 걸리는 시간일 수 있다. 네트워크를 통하는 균일하지 않은 지연을 모델하기 위해서 네트워크에서의 패킷 지연은 임의 값 T(N)로 정의하고 N노드를 가지는 네트워크 사이즈에 의존한다고 가정한다. 또한 패킷 프로세싱에 소요되는 시간은 실제 프로세서의 로드에 따라 달라질 수 있지만, 일반적으로 상수로 처리한다.

3. 정책기반 네트워크 구조의 평가

PBNM 구조에서는 정책 프로비저닝의 수행은 임의의 이벤트 요청을 받거나 새로운 정책을 적용할 때 발생할 수 있다. 이벤트는 PBNM에서 사용되는 응용에 따라 장애 관리, SLA 관리, 보안 관리, 스케쥴 관리에 관련된 속성을 가질 수 있다. (그림 1)의 1.a ~ 1.c경우와 같이 임의의 노드에서 특정 정책의 변화를 요청하는 이벤트를 발생할 수 있다. 1.a는 정적 정책 프로비저닝 방식으로서 정책이 생성된 이후에는 우리가 고려하는 동적 프로비저닝의 처리속도에 포함될 수 있다. 임의의 정책 노드에서 PDP로 새로운 정책을 요구하는 이벤트 발생률은 λ의 비율을 가지는 포아송 프로세스

로서 발생하는 것으로서 가정하였다. 즉, λ 는 정책 프로비저닝을 요구하는 서비스 요청과 NMS 등을 통한 이벤트에 의해 발생하는 정책 요청 빈도이다. 네트워크에서 상태 변화나 서비스 요청 시그날링을 통한 정책 적용이 요구될 때 프로비저닝에 영향을 주는 메트릭은 아래와 같다.

T_i : 정책 프로비저닝을 위한 평균 처리시간

U_i : 정책 프로비저닝을 위한 PDP 평균 처리 이용률

C_i : 정책 프로비저닝으로 PDP에 발생하는 평균 트래픽 량

G_i : GCD 에 소요되는 평균 처리 시간

3.1 1&2 계층 정책 구조(Single and Two-Tiered Policy Architecture ; S&TT)

1계층과 2계층 정책 구조는 PDP가 장비내부에 포함되어 있는 구조로서 같은 모델로서 고려한다. 따라서 PDP는 ANL을 수용하지 않는 노드들에 대하여 원격의 중앙 집중형 형태로 구성되거나 각 장비가 ANL을 포함하는 구조를 가지고 구성될 수 있다. PBNM 모델에서는 <표 1>에서 기술하는 인자들에 의해서 정책 프로비저닝 성능을 고려할 수 있다.

프로비저닝은 PDP로부터 PEP로 정책이 전송되어 해당 장비에서 서비스를 제공할 때까지 소비되는 시간을 의미한다. 정책 프로비저닝이 발생할 때, PDP에서 Q개의 정책을 조회 후(Sd), 해당 정책에 대하여 PEP에서 인식 할 수 있도록 PIB형태로 변환과정을 거친다(Pd), Q개의 정책 중에서 Q_n번째에서 해당 정책을 찾을 확률로서 $P(Q_n) = (Q-Q_n)/(Q+1-Q_n)$이라고 가정할 때, Q개의 정책에 대한 조회시간으로는 평균 Q/2가 걸릴 것이다[23].

〈표 1〉 PBNM 메트릭에 대한 성능 인자

인자	설명
Iq	PDP 와 PEP 사이에 요청 메시지 사이즈
Ir	PDP 와 PEP 사이에 응답 메시지 사이즈
Tc	정책 응답,요청에 대한 PDP에서의 처리시간
Tq	PEP에서의 정책 요청 처리시간
Tr	PEP에서의 정책 응답 처리시간
Sd	PDP 에서 정책을 조회할 때, 평균 조회시간 (=Q/2)
Pd	PDP로부터 PEP가 인식할 수 있는 정책 변환에 대한 평균 처리 시간
Td	PDP로부터 PEP로 데이터 전송 처리시간
Pe	PEP에서 디바이스가 인식 가능한 정책으로 변환과 적용 처리 시간
Sp	정책 충돌 감지에 걸리는 평균 시간 (= kQ^2)
h	메시지의 헤더 사이즈

또한 PEP에서는 정책을 장비가 인식 가능한 형태로 변환(Pe)하고 적용하게 된다. PDP에서는 해당 정책에 대하여 현재 적용된 정책들과의 충돌여부(Sp)를 검사하게 된다. PIB에 저장된 정보들에 대하여 충돌 감지에 걸리는 시간은 k개의 독립된 속성 타입을 가지는 Q개의 정책에 대하여 평균 $O(kQ^2)$의 조회 시간(Sp)이 수행될 수 있다[23].

S&TT 구조에서는 한 장비 내에 PDP와 PEP가 함께 위치하기 때문에 PBNM 모듈 간에 전송 처리시간과 전파시간(Propagation Time)은 포함되지 않는다. 식 (1)은 네트워크에서 정책을 요구하는 이벤트가 발생했을 때, PDP로부터 PEP에 정책이 적용되기까지 소요되는 시간이다.

$$T_1 = Pd + Pe + kQ^2 \quad (1)$$

임의의 네트워크 노드에서 이벤트가 발생할 때, PEP로부터 해당 정책에 대한 요청이 PDP로 전송된다. 이때 PDP에서는 정책을 조회하고(Sd), 조회된 정책에 따라 정책충돌 감지를 수행하게 된다(Sp). 그 후 해당 정책에 대하여 PIB로 변환(Pd) 과정을 거쳐 PEP로 전송하게 된다. 내부에 PBNM 모듈을 포함하기 때문에 메시지에 대한 처리시간은 포함되지 않는다. 식(2)는 임의의 이벤트가 발생하였을 때 PDP에서 이를 처리하여 정책 프로비저닝 하는데 소요되는 PDP 처리 이용률을 나타낸다.

$$U_1 = \lambda\left(\frac{Q}{2} + Pd + kQ^2\right) \quad (2)$$

S&TT 구조에서는 PBNM 모듈이 한 노드에 모두 포함되기 때문에 정책의 프로비저닝 시에 발생되는 트래픽은 없다. 그러나 노드 간에 정책 충돌 검출을 수행할 경우 발생되는 트래픽을 평가할 수 있다. 특정 노드에서 변경된 정책에 대하여 PDP를 포함한 다른 노드들에 정책 충돌 검출을 수행해야 한다면, N-1개의 노드에 대하여 라운드 로빈 방식의 순차적 수행을 한다고 가정한다. 우리는 트래픽 산정에 대하여 모니터링을 위한 NMS 트래픽은 고려하지 않는다. 그러므로 PBNM 발생 트래픽 량은 NMS로부터 경고나 유입 트래픽에 의한 정책 요청 이벤트만을 통하여 발생하는 제어트래픽을 고려하였다. 개별정책은 같은 크기를 갖는다고 가정할 때 다음과 같은 트래픽을 산출하게 된다.

$$C_1 = (N-1)\ \lambda\,(Iq + i \times Ir + 2h) \quad (3)$$

동일한 관리 도메인 내에서 정책에 대한 일관성을 유지하기 위해서 정책의 충돌과 해결을 수행해야 한다. S&TT 구조의 경우 같은 장비 안에 PEP와 PDP가 함께 존재하는 단일 시스템 기반의 제어구조를 가진다. 따라서 개별 도메인에 속하는 PDP들이 GCD를 고려해야하는 구조는 아니다. 그러나 본 논문에서는 네트워크의 규모의 확장과 정책 충돌을 다른 모델과의 성능 비교 측면에서 S&TT에서의 GCD를 고려해보았다. 따라서 S&TT구조의 단일 도메인 환경에서 독립적으로 동작하는 다른 PDP간에 정책 충돌 감지절차를 고려하였다.

(그림 3)에서는 PBNM모델에 따른 충돌 해결 과정에 대하여 보여주고 있다. S&TT구조(a)에서 보여주는 바와 같

이, N개의 네트워크 규모에서 특정 PDP는 임의의 노드로부터 정책의 정책 변화 요청이나 새로운 정책이 생성될 때, (N-1)개 다른 노드들과 정책 충돌 검출을 수행해야 한다. 이 때 정책 충돌 검출에 대한 요청과 응답에 대한 평균 전파시간은 2T(N)이 소요된다. 또한 요청과 응답에 대하여 각 노드에서 처리시간(Tc)과 응답 메시지에 대한 처리시간(Tq + Tr), 그리고 정책 충돌 검출 시간(Sp)이 소비된다. 따라서 개별 노드들에 대한 정책 검증 수행시간은 식(3) 과 같이 순차적으로 수행할 경우 아래와 같이 나타난다.

$$G_1 = (2T(N) + 2Tc + Tq + kQ^2)(N-1) \quad (4)$$

3.2 3 계층 정책 구조(Three-Tiered 정책 Architecture ; TT)

TT 모델에서는 N규모의 네트워크를 L개의 개별 PDP가 서브 네트워크로 분할하여 N/L개 노드들에 대하여 정책 프로비저닝을 수행한다. 각 PDP는 다른 관리 도메인을 구성할 수 있기 때문에 전송 메시지에 대한 보안헤더(Hs)를 고려한다. 보안 헤더는 IPSec과 같은 전송 데이터에 대한 기밀성, 무결성, 인증 기능을 제공하는 기능을 수행한다. 만약 L=1일 경우 보안 헤더는 고려하지 않을 수 있다. 따라서 Hs는 패킷당 보안 헤더의 오버헤드를 의미하고, 부가적인 처리 지연으로서 Ts는 각 노드에서 암호와 인증을 처리하는 비용이다. PDP가 새로운 정책을 프로비저닝 할 때, S&TT 구조의 처리시간인 식(1)보다 PDP로부터 PEP까지의 정책 전송시간과 보안헤더에 대한 처리시간 그리고 전파시간을 포함한 비용(Td + T(N/L) + 2Ts)과 PEP와 PDP간 요청에 대한 응답처리시간(Tq + 2Tc + Tr)을 부가적으로 포함한다. 따라서 새로운 정책을 프로비저닝 할 때, 어떤 이벤트에 의한 정책 프로비저닝은 PEP로부터 정책 프로비저닝 대한 처리시간(Sd + Pd + Td + T(N/L) + Pe + 2Ts + Sp)이 요구된다.

$$T_2 = Tq + 2Tc + Td + Pe + \frac{Q}{2} + Pd + T(\frac{N}{L}) + 2Ts + Tr + kQ^2 \quad (5)$$

PEP로부터 정책 요청이 발생하였을 때 프로비저닝 하기 위해서 PDP로부터 PEP로 정책이 전송된다. TT 구조에서는 정책 프로비저닝 시에 (2)에 비하여 PDP로부터 데이터 전송 처리 과정이 포함된다. 즉 PEP로의 데이터전송시간(Td)과 요청 메시지에 대한 처리시간(Tc)이 부가적인 오버헤드로 발생한다. 또한 보안 헤더에 대한 암/복호화 처리시간(Ts)이 더해진다.

$$U_2 = \lambda \frac{N}{L}(2Tc + Td + \frac{Q}{2} + Pd + 2Ts + kQ^2) \quad (6)$$

정책 프로비저닝 동안 PDP와 PEP사이에 평균 트래픽 량은 i개의 정책이 프로비저닝 된다면, $(i \times Ir + h)$크기의 트래픽이 발생한다. 반면에 PEP로부터의 질의와 i개의 정책에 대한 요청과 응답 메시지의 헤더에 대하여 $N(L \geq 1)$개의 노드로부터 트래픽이 발생$((N/L)\lambda(Iq + i*Ir + 2h)$할 수 있다. 본 논문에서는 특정 PDP에서 GCD발생률을 고려하기 위해서 다른 PDP로부터 발생되는 트래픽은 고려하지 않았다. 다중 PDP가 개별적인 관리도메인을 구성할 경우 안전한 통신을 위해 IPSec을 적용하게 되며, 보안헤더(Hs)로 인한 오버헤드를 가지게 된다.

$$C_2 = \lambda N(Iq + i \times Ir + 2h + 2hs) \quad (7)$$

TT구조에서는 다중의 PDP가 구성될 수 있기 때문에 $L(L > 1)$개의 PDP간 GCD 과정이 요구된다. (그림 3)의 (b) 에서는 TT구조에서 충돌 감지 절차를 나타내고 있다. 이 때 L개의 다중 도메인간의 충돌 검출이므로 보안 헤더에 대한 처리시간(Ts)이 요구된다.

$$G_2 = (2T(\frac{N}{L}) + 2Tc + Tq + kQ^2 + Ts)(L-1) \quad (8)$$

3.3 혼합형 정책 구조

(Hybrid-Tired Policy Architecture ; HT)

HT구조에서는 LPDP에 프로비저닝에 해당하는 정책이 존재하느냐 여부에 따라서 처리시간에 영향을 줄 수 있다. 일반적으로 정책서버기능을 수행하는 PDP에 비하여 LPDP에는 포함하고 있는 정책의 수가 메모리 용량에 의해 제한될 수 있기 때문에 PDP에서 포함하는 정책의 개수(Q)보다 LPDP가 포함하고 있는 정책의 개수(q)가 같거나 적게 된다. 새로운 정책의 프로비저닝의 경우는 TT 구조에서 처리시간(Sd + Pd + Td + T(N/L) + Pe + 2Ts + Sp)과 동일하다. 그러나 외부 이벤트에 의한 정책 요구는 LPDP에 해당 정책의 포함 여부가 프로비저닝 성능에 영향을 미칠 수 있다. 따라서 LPDP의 정책 조회는 알고리즘에 따라 수행시간은 달라질 수 있으나 충돌 검출 단계와 같은 비교과정을 거치게 된다.

동적 정책 프로비저닝의 경우에 해당 정책이 PDP에 존재하지 않을 가능성이 있다. 따라서 이 경우는 적응적 정책 생성 알고리즘의 수행을 요구한다. 정책의 프로비저닝 시간은 PDP로부터 PEP로 적용될 때까지 시간이기 때문에 요구 정책을 찾았을 때는 바로 적용하고, PDP로부터는 정책 충돌 감지에 대한 검사 후 승인 메시지만을 받는다. LPDP에서 해당 정책을 찾지 못했을 경우는 PDP에서 새로운 정책에 대한 처리와 정책 충돌 검출에 대한 처리를 수행한 후 PEP에서 적용한다. 따라서 LPDP에 존재할 확률을 $P_{Probability}$라 할 때 처리시간은 아래와 같이 나타난다.

$$\begin{aligned} T_3 = {} & P_{Probability}\{(\frac{Q}{2} + Pd + Pe)\} \\ & + (1 - P_{Probability})\{\frac{Q+q}{2} + Td + Pd + Pe + T(\frac{N}{L}) \\ & + 2Ts + kQ^2 + Tq + Tr + 2Tc\}(Q \geq q) \end{aligned} \quad (9)$$

HT 구조의 경우, LPDP에서의 정책 참조 율에 따라 PDP의 처리효율에 영향을 받을 수 있다. 개별적인 LPDP의 처리율은 PDP의 성능에 직접적으로 영향을 주지 않기 때문에

고려하지 않는다. LPDP에서 정책이 참조 되었을 때, PDP에서는 GCD를 수행하지 않고 정책 유무 검사만을 요구한다.

$$U_3 = \lambda \frac{N}{L}\{ P_{Probability}(2Tc+\frac{Q}{2}+2Ts) + (1- P_{Probability})(\frac{Q+q}{2}+2Tc+Td+Pd+2Ts+kQ^2\} \quad (10)$$

TT구조에서는 정책 프로비저닝 과정에서 항상 GCD를 수행하게 된다. 트래픽 발생량에 있어서도 마찬가지로 LPDP에 해당 정책이 존재할 확률 $P_{Probability}$에 의해 프로비저닝 수행 트래픽 발생에 영향을 받게 된다. 또한 LPDP에 해당 정책이 존재하지 않을 경우 해당 PDP로부터 GCD 과정에서 트래픽이 추가로 발생하게 된다.

$$C_3 = \frac{N}{L}\lambda\{ P_{Probability}(Iq+Ir+2h+2hs) + (1- P_{Probability})(L(2h+2hs+Iq+i_x Ir) + (1-i_x Ir))\} \quad (11)$$

(그림 3)에서와 같이 GCD에 소요되는 처리 절차는 TT 구조와 동일하다. LPDP에서 정책의 참조 확률에 따라 GCD를 수행하고 정책을 적용하는지 여부가 결정될 수 있다.

$$G_3=(1- P_{Probability})(2T(\frac{N}{L})+2*Tc+Tq+kQ^2+Ts)(L-1)) \quad (12)$$

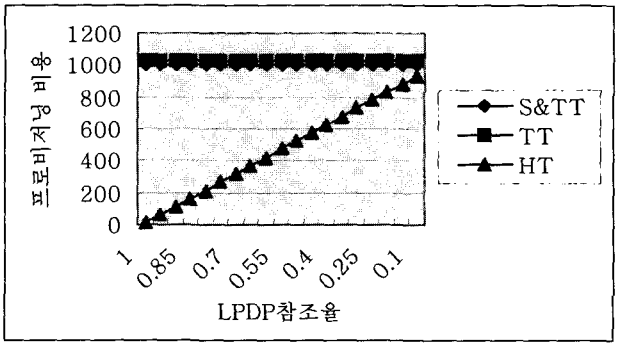
4. 평가 결과와 분석

PBNM모듈을 포함한 노드는 처리능력과 충분한 대역폭을 가진다고 가정할 때, 분산사건(Discrete-event) 시뮬레이션을 사용하여 (그림 2)의 접근 모델들의 성능을 비교하였다. 앞 절에서 살펴본바와 같이 PBNM 모델에 따라 프로비저닝시간($T_{1\sim3}$), PDP 이용률($U_{1\sim3}$), PDP관리 도메인에서의 트래픽 량($C_{1\sim3}$), 전역 충돌 감지($G_{1\sim3}$)에 대한 비용을 비교하였다. 각 모델간 같은 메트릭을 구성하는 인자들에 동일한 임의의 초기 값을 할당하고 점진적으로 증가시키면서 메트릭의 성능 변화를 관찰하였다. 특히, 다양한 인자들 중에서 PDP의 관리 노드에 영향을 주는 서브 도메인수(L), 관리 대상 네트워크 노드의 수(N), LPDP의 참조율은 모델간 성능메트릭에 상대적인 영향을 주는 인자로서 나타났다.

4.1 프로비저닝 비용

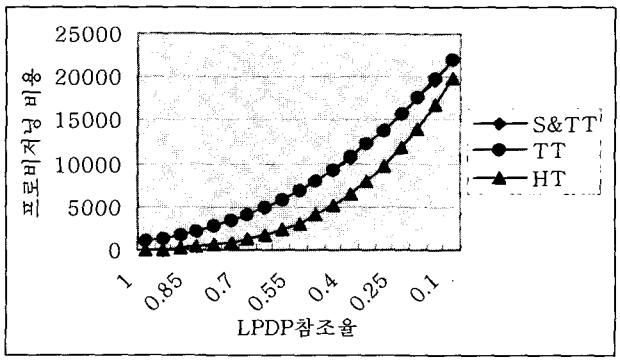
다중 PDP환경에서 프로비저닝 시간에 영향을 주는 요소는 PDP에 의해 분할되는 서브 관리 도메인수에 의한 평균 전파시간이 처리비용에 영향을 미친다. 즉, 정책 프로비저닝이 수행될 때 싱글도메인(L=1)의 경우는 평균 전파시간으로 T(N)이 소비되고, 다중 도메인(L > 1)일 때는 평균 T(N/L)의 시간이 걸리게 된다. 또한, PDP와 PEP의 분산구조에 의해 PBNM 통신간 오버헤드 비용으로서 모듈간의 전송 처리시간(Tq+2Tc+Tr+Td)과 L개의 서브관리도메인 간의 통신에 보안 채널을 구성하기 위한 처리비용(2Ts)이 소비되고 있다.

특정 노드에 어떤 정책을 프로비저닝할 때, S&TT 구조에서는 하나의 노드 내부에 PDP와 PEP가 위치하기 때문에 PBNM 모듈간 메시지 전송처리비용이 요구되지 않는다. 그러나 TT구조는 PDP와 PEP의 분산구조를 가지기 때문에 ($\triangle_1$= Tq+2Tc+Tr+Td+2Ts +T(N/L))의 비용만큼 메시지 전송 처리시간이 더 요구된다.



(그림 4) LPDP 참조율에 따른 프로비저닝 비용

(그림 4)에서는 HT의 LPDP 참조율에 따른 프로비저닝 비용을 다른 모델과 비교하여 나타내고 있다. LPDP가 프로비저닝에 해당하는 정책을 보유하고 있을 때 높은 참조율을 갖는다. 참조율이 높을 때 다른 모델에 비하여 HT가 비용이 적은 것은 PDP에서 처리되는 정책 충돌 감지시간과 PDP와의 메시지 전송처리비용이 포함되지 않기 때문이다. 그러나 참조확률이 낮아짐에 따라 다른 두 모델의 비용과 같아지는 것을 보여주고 있다. S&TT와 TT간의 비용 차는 $\triangle_1$에 의한 비용임을 보여주고 있다.

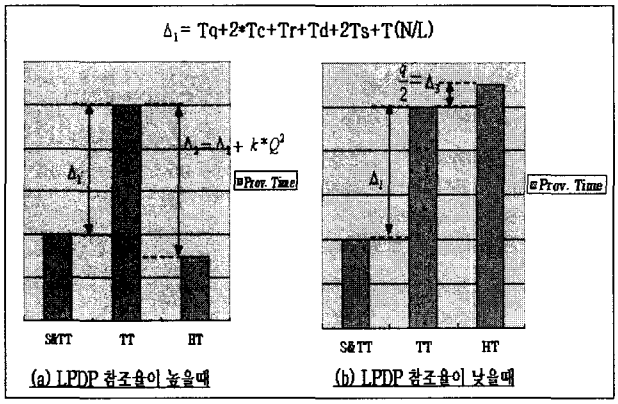


(그림 5) LPDP 참조율에 따른 프로비저닝 비용

(그림 5)에서는 정책의 개수(Q)와 속성의 개수(k)가 증가할 때 참조율에 따른 모델간 프로비저닝 비용의 상관관계를 보여주고 있다. 시뮬레이션을 통해서, 프로비저닝 비용뿐만 아니라 PDP이용률(4.2절)에서도 PDP에 저장된 정책의 개수(Q)와 정책의 속성의 개수(k)가 증가함에 따라 해당 정책의 조회와 로칼 정책 충돌에 대한 처리시간으로 인해 처리비용이 지수적으로 증가하고 있다. 따라서 관리노드와 사용자의 증가는 새로운 정책 생성을 요구하기 때문에 정책의 조회와 충돌검출에 요구되는 비용은 장치의 물리적인 처리능력 증

가 이외에도 개선된 조회와 검출 알고리즘을 통한 비용 축소가 요구된다.

(그림 6)에서는 HT구조의 LPDP 참조율에 따라 다른 구조에서 발생하는 프로비저닝 비용간의 상관관계를 보여주고 있다. HT와 TT구조의 프로비저닝 비용을 비교해 보면, HT에서 LPDP 참조율이 높을 때 TT구조보다 $\triangle_2 = \triangle_1 + kQ^2$ 만큼의 비용이 축소되고, 참조율이 낮을 때는 LPDP의 조회시간에 대한 비용($\triangle_3$=q/2)이 부가적으로 요구됨을 나타나고 있다.



(그림 6) 접근 모델에 따른 프로비저닝 비용

접근 모델에 따라 PBNM 프로비저닝 비용에는 PDP와 PEP간의 통신 처리($\triangle_1$), 정책 충돌 감지($\triangle_2 - \triangle_1$) 그리고 LPDP에 저장된 정책에 대한 평균조회시간($\triangle_3$)이 모델간의 프로비저닝 비용에 영향을 주는 인자임을 나타내고 있다. HT 구조의 관점에서 정책 프로비저닝 시간은 LPDP 참조율($P_{Probability}$)에 따라 다음과 같은 상관관계를 갖게 된다.

$$T3 = P_{Probability}(T1-(\triangle_2 - \triangle_1)) + (1-P_{Probability})(T2+\triangle_3) \quad (13)$$

따라서 PBNM 모델 사이에 전체 프로비저닝에 영향을 주는 시간은 LPDP조회 시간을 포함한 PBNM 모듈간의 통신비용과 PDP에서의 정책 충돌 감지 비용이 된다. HT구조는 네트워크 전체를 관리한다 하더라도 정책참조율에 따라 프로비저닝 비용에는 더 좋은 효율을 얻을 수 있음을 보여주고 있다.

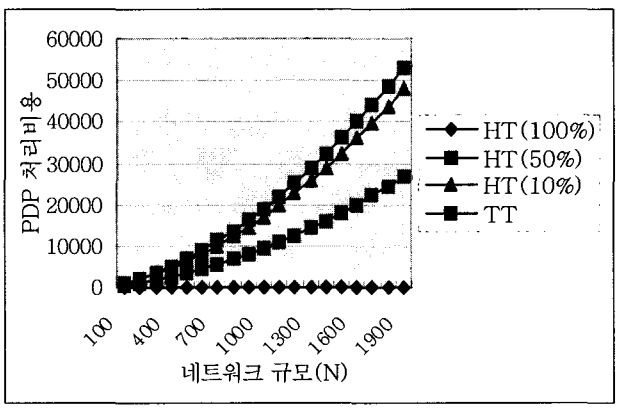
4.2 PDP 처리 비용

S. Liu의 NMS에서의 성능분석[1]의 경우, 전체적인 네트워크 구조를 효율적으로 관리하기 위해서 폴링 주기와 분산구조에 따라 NMS의 이용률이 영향을 받음을 제시하였다. PDP와 PEP의 분산구조로서 PBNM은 네트워크 관리뿐만 아니라 제어를 위해서 PDP의 이용률이 네트워크 제어 성능에 영향을 미치게 된다. 평가결과에서 PDP의 이용률은 네트워크 규모와 λ, 그리고 PBNM모델에 따라 성능의 차를 나타내고 있다. 이 때 PBNM 구조의 성능은 정책 요청에 대한 프로비저닝과 정책 충돌 검출을 수행하는 PDP의 능력에 의존하게 된다.

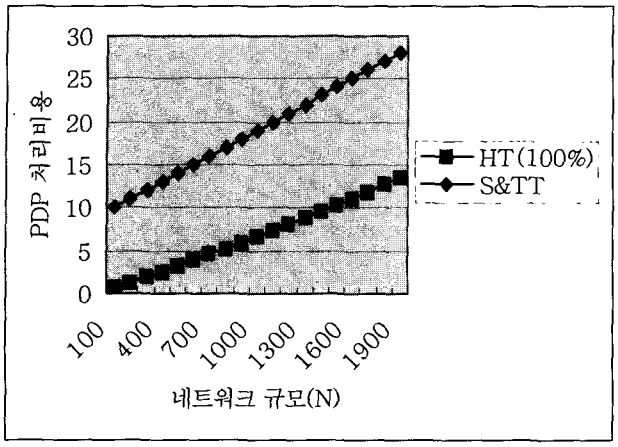
S&TT구조에서 PBNM 모듈간 정책 전송을 위한 처리과정은 없다. 그러나 PBNM 모듈을 탑재한 노드들 간에 정책 충돌 감지 수행은 그림 3.a와 같이 다른 PDP모듈사이에 통신처리를 요구할 수 있다. 만약 S&TT구조에서 PDP를 포함한 노드가 다른 (N-1) 노드에 대하여 λ 비율만큼 정책을 중앙 집중 관리한다고 할 때 (N-1)λ통신 회수와 통신비용(2Tc+Td)을 고려해야 하기 때문에 네트워크 사이즈와 이벤트 발생률(λ)에 의한 지수적인 오버헤드를 가져올 수 있다.

분산 구조인 TT 구조에서는 하나의 PDP가 N/L개의 노드를 제어한다고 할 때, 암호헤더 처리비용과 요청/응답 처리비용, 데이터 전송 처리시간이 소비되어 2Tc+Td+Ts 비용이 더 요구된다.

HT구조에서는 프로비저닝 비용에서와 마찬가지로 LPDP 참조확률에 따른 처리 이용률에 영향을 받게 된다. 평가 결과(그림7~10)에 따라, LPDP 참조율이 높을 경우, PDP 이용률은 HT $\leq$ S&TT < TT 순으로 비용이 산정된다. LPDP의 참조율이 낮을 경우는 S&TT < HT $\leq$ TT의 순으로 비용이 산정된다. (그림 7, 8)에서는 네트워크 규모 증가와 이에 따른 정책의 개수가 증가할 때 모델간 PDP의 이용률 관계를 나타내고 있다. HT구조에서 참조율이 낮을 때 이용률이 높은 것은 LPDP에서 해당 정책에 대한 조회 후 PDP에 다시 정책요청을 하며, 그 이후에 PDP가 해당 정책 조회와 정책 충돌 검사를 수행한 후에 다시 LPDP로 해당 정책을 전송하는 처리 과정을 수행하기 때문이다. HT구조의 LPDP 참조율이 높을 때, 다른 모델에 비해 가장 낮은 PDP 이용률을 보이는 것은 PDP로 정책요청 대신에 LPDP에서 참조된 정책에 대해 PDP가 승인 메시지만을 전송하기 때문에 오히려 S&TT 구조보다 적은 이용률을 갖게 된다. 이용률에 영향을 주는 인자들 중에서 변화량이 적은 노드간 데이터 전송에 처리되는 비용(2Tc+Td+Pd+2Ts)을 일정 상수(ϕ>0)로 가정하고, PDP 이용률이 일정하다 가정하면 PBNM은 수용가능한 정책의 수가 다른 성능 인자들에 대하여 아래와 같이 생성될 수 있다.



(그림 7) TT구조와 HT구조의 PDP 이용률



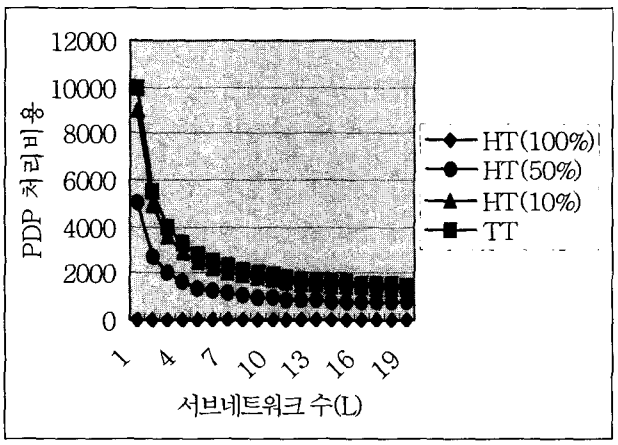
(그림 8) 9HT구조와 S&TT구조의 PDP이용률

$$Q = \sqrt{\frac{1}{k}(\frac{L}{\lambda N} - \phi)} \quad (L>0, \text{정수}) \qquad (14)$$

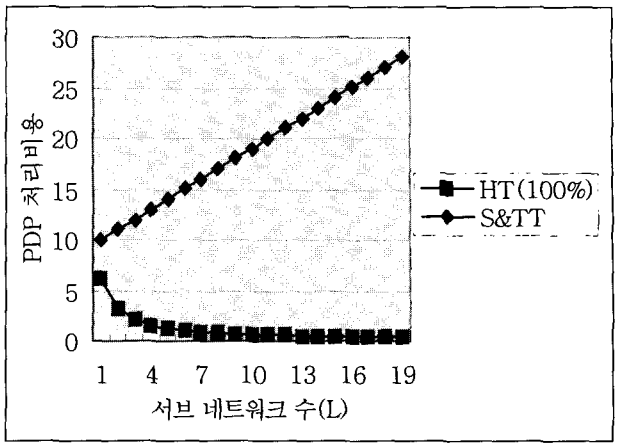
(그림 9, 10)에서는 일정한 네트워크 규모의 PBNM구조에서 서브네트워크(L)의 수가 증가할 때 PDP이용률에 영향을 보여주고 있다. 서브네트워크가 증가함에 따라 개별 PDP가 관리해야할 노드의 수가 N/L개로 줄어듦으로서 그 처리 이용률이 감소함을 나타내고 있다. S&TT구조는 단일 PDP 도메인을 가정하기 때문에 서브 네트워크의 개수에 영향을 받지 않음을 보여주고 있다.

4.3 발생 트래픽 량

PBNM이 NMS와 같은 네트워크 관리에 대한 구조라고 볼 때, 분산화 정도(N/L)와 λ에 의한 제어트래픽 발생은 하나의 PDP도메인에 영향을 주게 된다. 트래픽 발생량은 PBNM 모듈간 통신과정과 GCD과정에서 발생하게 된다. 하나의 관리도메인 내에서 L에 의한 PDP의 서브네트워크 분할의 의미는 개별 PDP가 관리해야할 PEP수의 감소를 의미하게 된다. L의 증가는 관리노드의 감소에 의한 정책 요청에 대한 트래픽 감소를 의미하게 된다. 그러나 L의 증가는 PDP 수의 증가에 의한 GCD 트래픽의 증가를 함께 야기한다.



(그림 9) TT구조와 HT구조의 PDP 이용률



(그림 10) TT구조와 HT구조의 PDP 이용률

TT구조에서는 L에 의한 관리 노드의 감소는 일정한 이벤트(λ) 발생률 환경에서 제어 트래픽 량의 상대적 감소를 나타낸다. 그러나 L이 1보다 클 때 PDP는 (L-1)개의 다른 PDP와 GCD를 수행과정에서 트래픽이 (N/L) λ(L-1)(Iq+ i ×Ir+2h)만큼 발생한다. 또한, 특정 PDP이외의 다른 PDP들에서는 개별적으로 (N/L) λ(L-1)만큼의 이벤트 발생률에 의해 GCD를 수행하게 된다. 따라서 본 논문에서는 GCD를 위해 개별 PDP가 라우드로빈 방식으로 (L-1)회 GCD를 수행한다 가정하였기 때문에 식(7)과 같이 L에 의한 영향을 받지 않게 된다. 즉 특정 PDP관점에서는 L에 의해 서브도메인의 발생 트래픽은 감소한다고 하더라도 GCD에 의한 트래픽 량의 증가로 인해 전체 트래픽 량은 영향을 받지 않는 결과를 가지게 된다.

하나의 정책 요청에 따라 다른 PDP노드들로 GCD를 요청하는 알고리즘의 수행 횟수(L-1)를 ω라 할 때, TT구조의 식 (7)에서 ω를 만족하는 GCD 수행 알고리즘을 유도할 경우 L에 의한 제어 트래픽은 감소하게 된다.

$$\omega \geq \frac{L}{N\lambda\phi} - 1 \qquad (L>1, \text{정수}) \qquad (15)$$

HT구조에서는 다른 메트릭과 마찬가지로 LPDP의 참조율에 따라 트래픽 발생에 영향을 받게 된다. 따라서 TT구조에서 발생하는 ω의 문제가 LPDP에서의 정책 참조율에 의해 트래픽 감소를 유도하고 있다. 식 (14)와 같이 LPDP로부터의 노드간 데이터 전송에 처리되는 비용(2Tc+Td+Pd+2Ts)을 일정 상수(ϕ_1>0)로 가정하고, LPDP에서 요청 정책을 참조하지 못했을 경우 데이터 전송 처리 비용을 상수(ϕ_2>0)로 가정했을 때 GCD를 수행하는 알고리즘 비용은 아래와 같이 나타난다.

$$\omega = \frac{1}{P_{probability}}(\frac{L}{N\lambda\phi_2} - 1 - P_{Probability}(\frac{\phi_1}{\phi_2} - 1)), \quad (\phi_1 \leq \phi_2) \qquad (16)$$

(그림 11)에서는 일정 네트워크 규모 하에서 서브네트워

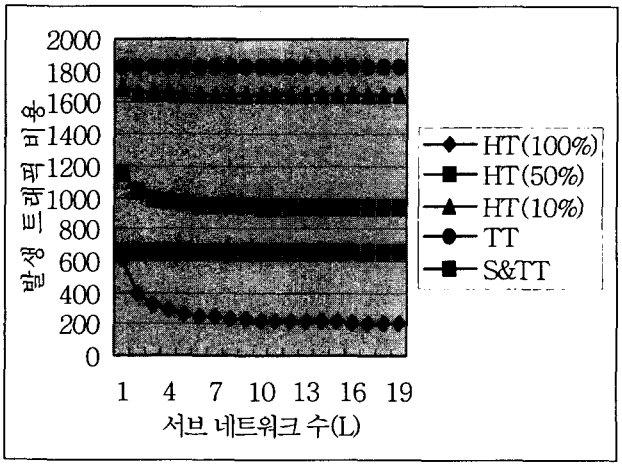
크 증가시 개별 PDP관리 도메인의 트래픽 발생률을 보여주고 있다. 그러나 서브네트워크의 수가 계속적으로 증가함으로 인해 발생 트래픽량이 일정 수준 이상에서 감소율이 낮아지는 이유는 각 서브네트워크를 관리하는 PDP간의 GCD 비용이 증가하기 때문이다. 즉, 서브네트워크의 증가는 일정 L까지는 관리노드의 제어 트래픽량을 감소할 수 있지만 일정 L이 증가하면서 각 PDP는 $(N/L)\lambda$의 발생률로 GCD를 (L-1)번 수행하기 때문에 제어트래픽이 증가하게 된다. 식 (16)에서 나타나는 바와 같이 LPDP참조율($P_{\text{Probability}}$)이 높을 경우, GCD 수행 알고리즘 횟수는 줄고, 참조율이 낮을 경우 수행 횟수는 증가하게 된다.

트래픽과 HT 구조의 LPDP참조율의 관계에서는 HT의 LPDP 참조율이 높을 경우, S&TT < HT ≤ TT 순으로 비용이 산정되고, 참조율이 낮을 경우 HT ≤ S&TT < TT로 평가된다. (그림 11)에서 S&TT비용이 일정 트래픽량을 보여주고 있는 것은 단일 PDP 도메인을 가정하였기 때문에 GCD를 수행하지 않기 때문이다.

4.4 전역 충돌 감지

우리가 각 모델에 따라 평가한 메트릭들 중에서 프로비저닝과 PDP 이용률은 GCD를 고려하지 않은 비용이다. 그러나 PDP도메인당 발생하는 트래픽 량은 GCD의 영향을 고려하였다. 본 논문에서 고려하고 있지는 않지만 GCD가 수행되고 정책충돌이 발생하였을 때는 몇 가지 기준을 통해서 정책 충돌 해결을 수행해야 한다. GCD 처리에 소요되는 비용은 전체적인 프로비저닝 시간, PDP 이용률 그리고 PDP로의 발생 트래픽 량에 영향을 주게 된다.

(그림 2)에서와 같이 LCD의 경우는, 네트워크 전체를 제어하기 위해서 PDP가 정책에 대한 일관성을 유지해야 하기 때문에 분산 PBNM구조라 하더라도 PDP가 개별 PEP들에 대한 LCD를 수행하게 된다. 하나의 특정 PEP 노드에 요구되는 서비스를 제공하고, 이때 PDP에 의해 관리되는 다른 PEP들에 프로비저닝된 정책들과의 일관성 여부를 검증해야 한다.



(그림 11) PDP수 증가에 따른 트래픽 발생량

다중 도메인 환경일 경우나 다중 PDP로 구성된 S&TT응용 구조에서 GCD가 요구될 경우, PDP간에 충돌 감지 과정이 요구된다. 정적 정책 프로비저닝의 경우 GCD 처리에 소요되는 비용은 프로비저닝 이외에 요구되는 시간으로서 PBNM구조에 따라 별도로 산정될 수 있다. 그러나 동적 적응형 정책 제공 방식의 경우 정책 프로비저닝 비용은 GCD의 처리비용에 의해 영향을 받게 된다. 식 (12)에서는 다른 메트릭에서와 마찬가지로 HT의 LPDP 참조율이 GCD비용에 주는 영향을 나타내고 있다. (그림 11)에서는 L의 수가 증가함에 따라 GCD의 비용에 의해 발생 트래픽 량에 영향을 받고 있음을 보여주고 있다. 따라서 동적 적응형 정책 제공 방식의 경우에 트래픽량 뿐만 아니라 프로비저닝 비용과 PDP 이용률의 메트릭에서도 LCD 과 GCD 그리고 충돌 해결에서 비용이 고려되어야 한다.

LPDP에서 정책 참조 성공은 PDP에도 이미 검증된 같은 정책 정보를 보유한다고 말할 수 있기 때문에 관리자의 정책에 따라 LPDP의 참조 성공시 GCD를 수행할지 여부를 결정할 수 있다. 그러나 네트워크 상태나 시그날링의 예외적인 조건에 의해 GCD를 수행해야 할 수도 있다. 그러나 다중 PDP환경의 TT 구조에서는 항상 새로이 프로비저닝이 요청되는 정책에 대해서 다른 PDP와 정책에 대한 충돌을 검증해야 하기 때문에 이러한 PBNM 응용 특성 하에서는 비효율적이다.

5. 결 론

본 논문에서는 정책 기반 네트워크 관리에 대한 중앙 집중 형태와 분산 형태의 모델을 비교하고 모델링하기 위한 분석적인 프레임워크를 제안했다. 정책기반 네트워크는 다양한 응용분야에서 도입되고 있다. 현재 다양한 PBNM에 대한 접근 방식들은 특정 모델에 의존한 응용개발에 치중하였었다. 많은 정책을 유지하고 관리하는데 있어서 PBNM 구조의 처리성능은 네트워크 관리와 제어에 있어서 중요한 인자가 된다. 처리성능은 정책 충돌과 해결, 정책의 적용 방식, 정책이 정의되는 응용의 특성 그리고 PBNM구조에 따라 영향을 미치게 된다. 각 모델은 평가 메트릭으로서 정책 프로비저닝 시간, 트래픽 발생량, PDP에서 처리율 그리고 GCD에 대해 평가하였다.

평가 결과에서 S&TT 구조는 단일 시스템구조에서 적합하나 다중 노드와의 정책 연합은 네트워크 규모에 의해 지수적인 처리시간의 증가를 가져온다. TT구조는 S&TT구조의 오버헤드를 PDP분산을 통해 해결할 수 있으나, 정책 충돌시 PDP의 분산도에 따라 통신비용을 가중하게 된다. HT 구조는 PEP에 포함된 LPDP의 참조율이 높을 경우 오히려 S&TT와 TT구조에 비하여 좋은 성능을 나타내고 있다. 본 논문에서 평가한 결과와 같이 각 구조는 응용 특성에 따라 장단점을 제공할 수 있다. 따라서 PBNM을 통한 서비스를 제공할 때 응용의 특성을 주의 깊게 평가하여 적절한 제어 구조를 설계하여야 한다. 또한 향후 응용 서비스의 요구사

항과 PBNM 구조간의 상관관계에 의한 분석과 모델링이 요구된다.

참 고 문 헌

[1] Thomas M. Chen, Stephen S. Liu, "A Model and Evaluation of Distributed Network Management Approaches", IEEE Journal on Selected Areas in Communications, VOL. 20, MAY 2002.

[2] Jude, M., "Policy-Based Management: Beyond the Hype", Business Communications Review, March 2001.

[3] G. Premkumar and P. Venkataram, "Artificial intelligence approaches to network management: recent advances and a survey", Computer Commun. Journal, Vol.20, No.4, 1997.

[4] QoS forum White Paper, "Introduction to QoS Policies", QoS Forum, July, 1999.

[5] Andreas Polyrakis, et. al., "The Meta-Policy Information Base", IEEE Network Journal, April, 2002.

[6] Emil Lupu, Morris Sloman, et. al., "An Adaptive Policy Based Framework for Network Services Management", Journal of Networks and Systems Management, September, 2003.

[7] Ribeiro, M.B., et. al., "An architecture to monitor QoS in a policy-based network", Conference Proceedings of ICT '03, March, 2003.

[8] Damianou, N., "A Policy Framework for Management of Distributed Systems", Ph. D. Thesis, February, 2002.

[9] Gai, S., et al. "QoS Policy Framework Architecture", draft-sgai-policy-framew ork-00.txt, February, 1999.

[10] K. Yoshihara, M. Isomura, et. al., "Distributed Policy-based Management Enabling Policy Adaptation on Monitoring using Active Network Technology", Conference Proceedings of DSOM '01, 2001.

[11] Nevil Brownlee, "Traffic Flow Measurement Architecture", IETF RFC2722, Oct., 1999.

[12] Marcial Porto Fernandez, et. al., "QoS Provisioning across a DiffServ Domain using Policy-Based Management", Conference Proceedings of GLOBECOM '01, 2001.

[13] P. Cremonese, M. Esposito, et. al., "A Framework for Policy-Based Management of QoS Aware IP Networks", Conference Proceedings of NETWORKING '02, 2002.

[14] Stylianos Gouveris., et. al., "Automated Management of IP Networks through Policy and Mobile Agents", Conference Proceedings of MATA '02, 2002.

[15] S. Boros, "Policy-Based Network Management with SNMP", Conference Proceedings of the 6th Eunice Summer School, Netherlands , September 2000.

[16] Corrente, A., et. al., "Policy provisioning performance evaluation using COPS-PR in a policy based network", Conference Proceedings of Integrated Network Mana- gement, 2003.

[17] R. Yavatkar, et. al., "A Framework for Policy-based Admission Control", IETF RFC 2753, January, 2000.

[18] K.L. Eddie Law, Achint Saxena, "Scalable Design of a Policy-Based Management System and Its Performance", IEEE Communications Magazine, 2003.

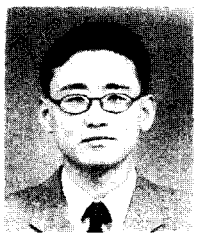
[19] Thi Mai Trang Nguyen, "COPS-SLS usage for dynamic policy-based QoS management over heterogeneous IP networks", IEEE Network Journal,17,2003.

[20] K. Chan, et. al., "COPS Usage for Policy provisioning" (COPS-PR), IETF RFC 3084, March, 2001.

[21] Fu, Z., Huang, H., Loh, K., Gong, F., Bladine, I., Xu, C., "Ipsec/VPN Security Policy: Correctness, Conflict Detection and Resolution", Conference Proceedings of Policy'01, January, 2001.

[22] Nicole Dunlop, et. al., "Dynamic Conflict Detection in Policy-Based Management Systems", Conference Proceedings of EDOC '02. IEEE, 2002.

[23] Verma, D.C., "Simplifying network administration using policy-based management", IEEE Netwrok Journal, 2002.



임 형 진

e-mail : hjlim@imtl.skku.ac.kr

1998년 한림대학교 컴퓨터공학과(학사)

2001년 성균관대학교 정보통신공학과(석사)

2003년~현재 성균관대학교 컴퓨터공학과 박사과정

관심분야 : IPv6, NEMO, PBNM, Mobile AAA, VPN, Multicast Security

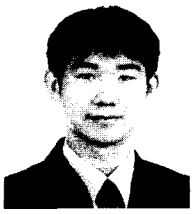
이 현 주

e-mail : hjlee98@imtl.skku.ac.kr

2004년 성균관대학교 화학공학, 정보통신공학부(학사)

2004년~현재 성균관대학교 컴퓨터공학과 석사과정

관심분야 : 네트워크 보안, AAA, IPv6, 이동 컴퓨팅, GRID 네트워크



이 종 혁

e-mail : jhlee@imtl.skku.ac.kr
2004년 대전대학교 정보시스템공학과(학사)
2004년~현재 성균관대학교 컴퓨터공학과 석사과정
관심분야 : 네트워크 보안, 이동 IPv6, AAA, PBNM

정 태 명

e-mail : tmchung@ece.skku.ac.kr
1981년 연세대학교 전기공학과(학사)
1984년 일리노이 주립대학 전자계산학과 (학사)
1987년 일리노이 주립대학 컴퓨터공학과 (석사)
1995년 퍼듀 대학 컴퓨터공학 (박사)
1984년~1987년 Waldner and Co., System Engineer
1987년~1990년 Bolt Bernek and Newman Labs. Staff Scientist
1995년~현재 성균관대학교 정보통신공학부 정교수
관심분야 : 실시간시스템, 네트워크 관리, 네트워크 보안, 시스템 보안, GRID 네트워크, 전자상거래