情報保護學會論文誌
第18卷 第5號, 2008. 10

신뢰도가 낮은 네트워크 환경을 위한 트리 구조 기반의 권한 관리 기법

양 수 미
수원대학교

Privilege Management Technique for Unreliable Network Environments based on Tree Structure

Soomi Yang
The University of Suwon

요 약

ISO/IEC 9594-8은 공개키 인증서 프레임워크와 속성 인증서 프레임워크를 정의하고 있다. 속성 인증서 프레임워크에서 권한 관리 기반 구조(PMI)를 다루고 있다. 권한 관리 기반 구조에서는 권한 관리를 위하여 속성 인증서를 사용함에 있어서 권한의 할당 및 명세를 독립적으로 하기 위하여 역할 할당 인증서와 역할 명세 인증서를 사용한다. 역할 명세 인증서는 권한의 명세를 포함하며, 네트워크 환경의 권한 관리를 위한 내용을 담고 있다. 신뢰도가 낮은 네트워크 환경의 권한 관리는 잠재적으로 장애가능성이 있는 노드와 에지를 포함하는 환경에서 권한 정보 전송의 신뢰성과 효율성을 얻고자하는 것이다. 각 노드는 수집된 역할 명세 관계 정보를 기반으로 하여 계층적으로 연결된 역할 명세의 권한 구조 트리를 구성한다. 본 논문에서는 역할 명세 인증서의 트리 구조화를 통한 권한 관리 비용을 계산하고 권한의 생산 및 갱신에 따른 오버헤드를 줄이도록 한다. 규모 확장성을 위해 멀티캐스팅 패킷을 사용하며, 네트워크 통신의 패킷 손실률과 네트워크에 참가 및 이탈을 반복하는 컴퓨팅 노드의 신뢰도를 감안하여 관련 성능을 분석하여, 제안된 구조의 권한 관리 기법이 보다 나은 성능을 가짐을 보인다.

ABSTRACT

IISO/IEC 9594-8 defines the public key framework and attribute certificate framework. Attribute certificate framework deals with privilege management infrastructure(PMI). In PMI, for privilege management using attribute certificates, role assignment certificates and role specification certificates are used to assign and specify privileges independently. Role specification certificates includes privilege specifications and the details for privilege management of network environments. Privilege management of unreliable network environment tries to enhance the reliability and efficiency of privilege information transmission forwarding over unreliable routes in the presence of potentially faulty nodes and edges. Each node forms a role specification tree based on role specification relationship data collected from the network. In this paper privilege management cost with the role specification certificates tree structure is evaluated trying to reduce the overhead incurred by role creation and modification of privileges. The multicasting of packets are used for scalability. We establish management cost model taking into account the packet loss and node reliability which continuously join and leave for network. We present quantitative results which demonstrate the effectiveness of the proposed privilege management scheme.

Keywords : Privilege Management, Attribute Certificates, Network Reliability

Ⅰ. 서 론

컴퓨팅 활동이 매우 유동적이어서 네트워크에 참가 및 이탈을 반복되는 환경에서 사용자 권한 인증을 위한 권한 정의도 동적인 네트워크 상에 분산되어 있어서 이를 효율적으로 적용할 기술이 필요하다. 이에 역할기반 접근제어를 역할 할당과 역할 명세를 독립적으로 정의하여 융통성을 부여하고 유연한 네트워크 환경을 고려한다면 특화된 보안구조로서 좋은 방안이 될 수 있다. X.509에는 기존의 공개키 기반 구조 PKI (Public Key Infrastructure)를 위한 공개키 인증서 PKC (Public Key Certificate)에 추가하여 권한 관리 기반 구조 PMI (Privilege Management Infrastructure)를 위한 속성 인증서 AC (Attribute Certificate)가 포함되었다[1,2,13, 14]. 속성 인증서를 이용한 역할기반 접근제어에 있어서 속성 인증서를 역할 할당 인증서와 역할 명세 인증서로 사용할 수 있다. 이는 보다 융통성있는 권한 관리가 가능하도록 한다.

근래에 대두되고 있는 유비쿼터스 컴퓨팅 환경이나 P2P 오버레이 네트워크 환경은 대규모의 유무선 네트워크로 연결된 컴퓨터가 중앙의 제어 없이 자율적으로 상호 작용하는 동적 환경으로 대표된다. 중앙의 통제가 없을 뿐 아니라, 응용이 완결되지 않은 채 접속이 종료되는 컴퓨팅 노드들로 인하여 전체적으로 정리된 네트워크 자원 구조가 유지되지도 않는다. 이러한 분산성을 유지하면서 시스템간의 관계를 정의하여야 한다. 반면에 사용자는 어느 시점, 어느 장소에서든지 자원과 서비스에 접속할 수 있기를 기대한다. 이를 지원하기 위해서 자원을 누구에게나 접속 가능하도록 가용성을 제공해야 하는 경우, 오픈된 네트워크 환경의 보안을 고려하기 위해서는 중앙의 통제 없이 사용자의 인증과 접근제어를 이룰 수 있어야 한다. 이를 위해 분산된 신뢰 구조(trust structure)가 제안되었다[3]. 분산된 신뢰 구조에서는 역할기반 접근 제어를 하며 권한 위임 기법을 쓴다. 본 논문에서는 분산된 신뢰구조의 철학을 속성 인증서를 이용하는 권한 관리 구조 관리에 적용, 역할 명세 인증서 간의 신뢰구조를 확립한다. 여기에는 무작위로 생성, 삭제되는 노드 고장률과 특히 무선망에서 고려되어야할 패킷 손실률로 인한 네트워크의 낮은 신뢰성이 문제가 된다. 노드 고장률에 비례하는 메시지 손실률과 망의 품질에 반비례하는 패킷 손실률이 권한 관리 구조의 유지와 권한 정보 전달의 오버헤드로 작용한다. 이를 낮추어 신뢰성을 높기 위해서는 권한 관리 구조의 효율적 구성이 필요하며, 권한 관리 구조 내에서 전달되는 데이터의 전송 효율을 높여야한다. 본 논문에서는 역할 명세 인증서의 구조화로 권한 관리의 성능 개선을 추구하면서 패킷손실률을 보상하며 규모 확장성을 제공하는 멀티캐스팅을 도입하여 더욱 높은 성능 향상을 제공한다.

논문의 순서는 다음과 같다. 2장에서 권한 관리에 관한 관련 연구를 보고, 3장에서 분산 환경에서의 권한 관리에 관한 권한 명세의 기술, 분산된 권한 구조의 생성과 관리 기법 등을 기술한다. 4장에서 성능 분석 결과를 보이고, 5장에서 요약과 함께 결론을 맺는다.

Ⅱ. 관련 연구

2007년에 국가 표준으로 제정된 KS X ISO/IEC 9594-8[13]은 ISO/IEC 9594-8 : 1998/Cor 2 : 2002를 근간으로 하고 있다. ISO/IEC 9594-8[14]은 2005년도에 재개정되었으며 이의 내용은 공개키 인증서 기반의 개인 인증 프레임워크와 속성 인증서 기반의 권한 인증 프레임워크이다. 권한 정의를 위해서는 공개키 인증서를 사용할 수도 있으나 기능이 한정되어, 속성 인증서를 사용하는 권한 관리 프레임워크가 정의되었고[14], 이는 2001년에 제정된 [2]의 개정판이다. IETF에서도 유사한 내용이 rfc3281[1]로 제정되어있으며 현재까지 유효하다. 권한 인증의 기본은 역할 기반 접근 제어로 권한의 정의와 인증을 다룬다. NIST의 역할 기반 접근 제어 표준[4]과 그 뒤를 이은 많은 연구에서 여러 종류의 역할기반 접근제어 기법이 제시되었으나 역할 또는 권한 정의의 구조화를 통하여 성능 향상을 모색하고자 하는 시도는 없었다.

[3]에서는 중앙의 통제 없이 사용자의 인증과 접근제어를 하기 위해 분산된 신뢰 구조(trust structure)가 제안되었다. [5]에서는 시간에 따라 변화하는 동적 환경을 대상으로 권한 위임의 유연성을 제고하였다. [3]과 [5]는 기존의 PKI의 한계를 인식하여, 권한 관리를 위한 새로운 기법을 제시하였으나, 표준화된 속성인증서의 사용 등 보편적인 방식을 배제함으로써 적용범위를 한정하였다. [6,7] 에서는 Grid 환경에서 각 참여자의 권한 인증을 위하여 속성 인증서를 사용한다. Grid 환경

접수일 : 2008년 3월 10일; 수정일 : 2008년 5월 19일;
채택일 : 2008년 7월 4일
† 주저자 smyang@suwon.ac.kr

에서 자원과 사용자의 관계는 보다 임의적이고 동적이며, 같은 보안 도메인 안에 존재하지도 않으므로 체계적인 명명에 의한 명명자(identifier)에 의해 지명되거나 구분되지 않고 자신이 가진 속성에 의해 존재확인(identify)이 되므로, 속성에 기반한 접근제어가 각광받고 있다. 또한 전자상거래를 위한 보안구조의 하나로 사용자 인증과 권한 인증을 위한 기반구조(AAI, Infrastructures for Authentication and Authorization)[12]가 제안되어 있고, 속성에 기반을 둔 접근제어가 제시되어 있다[11]. 공개키 인증서에 속성을 담도록 확장하여 P2P 네트워크 상에서 권한 인증 및 접근제어를 하는 예가 [15]에 제시된 바 속성 인증서를 이용하여 더 나은 기능을 얻을 수 있다. 이렇듯 다양한 분산 환경의 여러 응용을 위한 융통성 있는 속성 인증서 기반의 권한 관리가 제안되어 있으나, 기존의 공개키 인증서 대신에 단순 속성 인증서를 사용하는 것만으로 얻는 용이함과 성능에 만족하고 있다. 속성 인증서를 구조화하여 융통성과 성능 향상을 얻을 수 있음을 간과하고 있다. 컴퓨팅 노드의 이동성으로 인한 지속적인 네트워크 참가 및 이탈 에 따른 노드 존재의 불확실성과 무선망으로 대표되는 낮은 신뢰도의 통신 네트워크에 대한 고려가 없으며 향후 권한 관리 영역이 지리적으로 넓은 범위를 차지함은 물론 대상 자원의 개수도 기하급수적으로 늘어나고 이동성이 극대화된 저사양의 컴퓨팅 노드도 늘어날 것으로 예상되는데, 이에 대비한 규모 확장성에 대한 고려도 없다.

Ⅲ. 분산 환경에서의 권한 관리

3.1 권한 명세의 기술

X.509는 공개키 인증서 PKC(Public Key Certificate)에 이어 속성 인증서 AC(Attribute Certificate)를 [그림 1]과 같은 형식으로 정의하였으며[1, 2, 14], ISO에서는 권한 관리 구조(PMI)에서 AC를 이용하는 역할 기반 접근 제어에 대해 기술하고 있다[2, 14]. 본 논문에서는 [1]과[13, 14]에 정의된 속성 인증서를 사용하는 권한 관리 프레임워크를 기반으로 한다. [그림 1]의 각 필드에서 holder는 속성 인증서의 소유자로서 공개키 인증서의 주체와 동일하며, attributes는 속성(역할 정보)를, extensions는 추가사항을 가진다. holder에 들어가는 속성의 주체나 attributes의 값은 속성 인증서를 역할을 주체에게 할당하는 역할 할당 인증서(Role Assignment

```
AttributeCertificate :: = SIGNED
                    {AttributeCertificateInfo}
AttributeCertificateInfo :: = SEQUENCE
    {version AttCertVersion, -- version is v2
    holder Holder,
    issuer AttCertIssuer,
    signature AlgorithmIdentifier,
    serialNumber CertificateSerialNumber,
    attrCertValidityPeriod AttCertValidityPeriod,
    attributes SEQUENCE OF Attribute,
    issuerUniqueID UniqueIdentifier OPTIONAL,
    extensions Extensions OPTIONAL }
```

(a)속성 인증서의 형식

```
roleSpecCertIdentifier EXTENSION :: =
    {SYNTAX RoleSpecCertIdentifierSyntax
        IDENTIFIED BY {id-ce-roleSpecCertIdentifier}}
    RoleSpecCertIdentifierSyntax :: = SEQUENCE
        SIZE (1..MAX) OF RoleSpecCertIdentifier
    RoleSpecCertIdentifier :: = SEQUENCE {
        roleName [0] GeneralName,
  roleCertIssuer [1] GeneralName,
  roleCertSerialNumber [2] CertificateSerialNumber
                                    OPTIONAL,
  roleCertLocator [3] GeneralNames OPTIONAL }
```

(b)역할 명세 인증서 식별자 extension의 형식

〔그림 1〕 ASN. 1으로 기술된 속성 인증서관련 형식

Certificate)와 역할에 대한 권한 명세를 가지는 역할 명세 인증서(Role Specification Certificate)로 구분하여 사용할 경우 다른 값을 가지게 된다. 역할 할당 인증서와 역할 명세 인증서를 구분하여 사용하여 권한을 관리하는 이유는 역할 할당을 변경하지 않고 역할에 대한 명세만을 정책에 따라 독립적로 바꿀 수 있도록 하여 융통성을 가지기 위함이다. 속성 인증서를 간략하게 그려 사용 예를 설명하면 [그림 2]와 같다. 주체 S_i 에게 권한(Privilege) P_i 를 직접 연결하지 않고 권한에 해당하는 역할(권한)명 R_i 를 중간에 두고, S_i 에게 간접적으로 P_i 를 할당 한다. R_i 에 대한 명세 P_i 를 역할 명세 인증서를 이용하여 독립적으로 정의함으로써, 향후 R_i의 명세가 P_i로 바뀌었을 때, 주체 S_i와 역할 R_i 간에 역할 할당 인증서로 지정된 역할 할당에는 아무 변화도 주지 않으면서 S_i가 가지는 권한의 내용을 역할 명세 인증서만 바꿈으로써 동적으로 바꿀 수 있는 것이다. 이와 같이 역할의 할당과 명세를 독립적으로 구현하기 위한 속성 인증서의 사용에 있어서 역할 명세 인증서를 쓸 경우, 역할 할당 인증서는 역할 확장 필드에 역할명 또는 역할 명세 인증서 식별자를 가진다. 역할 명세 인

holder	attributes	extensions
pkc subject S_i	역할 이름 R_i (공백 가능)	역할 명세 인증서 정보

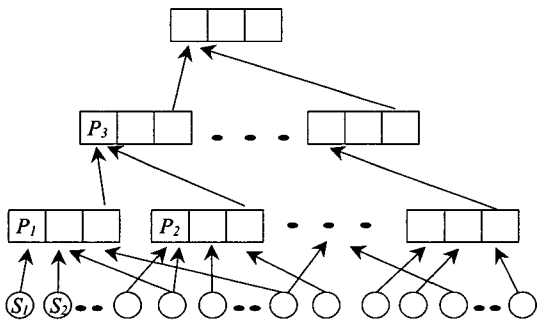
(a)

holder	attributes	extensions
역할 이름 R_i	역할 정보 P_i (공백 가능)	다른 역할 명세 인증서 정보

(b)

(a : 역할 할당 인증서 b : 역할 명세 인증서)

〔그림 2〕 간단하게 표현한 속성 인증서의 예



〔그림 3〕 역할 명세 인증서의 구조화

증서의 소유자(holder)는 역할 할당 인증서의 역할명(roleName)에 해당한다. 본 논문에서는 역할 명세 인증서의 역할 확장 필드가 다른 역할 명세 인증서의 정보를 가지도록 하여, [그림 3]과 같이 역할 명세를 구조화한다. 이는 역할 명세를 생성, 변경 및 제거함에 있어서 부분적인 정의를 다룰 수 있게 해주므로 역할 명세 관리의 융통성을 더욱 높여준다.

[14]에 ASN.1으로 기술되어 있는 속성 인증서의 최상위 데이터 형식은 [그림 1(a)]에 보인 바와 같다. extensioins의 영역이 차지하는 비중은 매우 가변적이기는 하나 대체로 전체의 10%이상이다. extensions 중에서 역할 명세의 구조화에 관여하는 역할 명세 인증서 정보 extension에 대한 내용은 [그림 1(b)]에 보인 바와 같다. extension 부분은 권한을 이루는 역할 정의의 갯수 n 에 비례해서 늘어난다. 역할 정의가 세분화되고 구조화되는 경우 이 영역의 크기를 1/n으로 줄일 수 있다. General Name과 GeneralNames는 다양한 스트링으로 정의되므로 줄어드는 크기의 값은 가변적이다. 역할 명세 인증서의 관리에서 주기적으로 전송하여야하는 데이터의 량은 권한 정보의 변화에 따른 역할 명세서와 제어 트래픽으로, 각 노드에서 발생되는 제어 트래픽은 노드 생성 및 변경에 따른 링크정보 테이블 갱신, 링크정보 테이블 유지관리 등 네트워크 구조관리를 위한 것과 PMI 유지에 필요한 것이다.

역할 명세가 연결된 경우 권한을 사용하고자 할 때 위의 역할 명세 인증서 체인을 따라가야 하므로 그에 따른 성능저하가 있을 수 있다. 그러나 역할 적용시의 오버헤드에 비해 역할 생성 및 갱신 시에 얻는 성능 상의 이익이 더 크다. 역할 적용시의 오버헤드는 캐싱으로 극복할 수 있으므로, 역할 명세의 구조화로 역할 생성 및 갱신 시의 오버헤드를 줄이는 것이 효율 개선에 더 많이 기여한다. (캐싱의 효율에 대한 논의는 본 논문의 범위를 벗어나므로 생략한다.) 구조화의 효율성을 정량적으로 보이는 것이 본 논문의 목적이라고 하겠다. 권한 명세가 구조화되어있지 않을 경우 역할의 적용이 하나의 단계로 이루어지는 장점이 있으나, 저장해야하는 권한 명세 인증서 크기가 늘어나며, 소규모 메모리를 가지는 유비쿼터스 환경의 무선 단말의 경우 사용에 제약을 받게 된다. 무선 단말의 증가에 따라 권한 명세의 구조화는 더욱 성능향상에 기여할 것이다.

3.2 분산된 권한 구조의 생성과 관리 기법

권한구조를 구성하고자 역할 명세 인증서가 체인을 이룰 경우, [그림 3]과 같은 트리 구조가 된다. [그림 3]에서 구조화의 예를 들면, subject S_1과 S_2는 권한 P_1과 P_2를 가지고 있는 것이다. 역할 명세 인증서는 구조화를 하지 않을 경우 단일 단계로 구성된 납작한 형태의 선형구조가 된다. 역할 명세가 구조화되면 역할 명세 인증서의 크기는 역할의 개수가 n일 경우, 역할 명세 부분이 1/n로 감소하게 된다.

역할 명세가 이루는 트리 구조의 구성요소를 보면, 전체 역할의 개수, R 에 대하여 최하위 역할 명세 인증서의 가능한 최대 개수, M 는 $\sum_{i=1}^{R} {}_R C_i$ 가 된다. (${}_R C_1$은 역할을 한 개 가지는 역할 명세 인증서이고, ${}_R C_R$은 모든 역할을 포함하는 역할 명세 인증서로서 전이 상태인 경우이외에 실질적 의미는 없다.) 트리의 높이를 h 라 할 때, 루트의 레벨은 0이고 단말의 레벨은 $h-1$이다. 각 노드는 공통의 역할을 가진 하위 노드에 대하여 차수 d 의 에지를 가진다. 총 하위 역할 명세 인증서 개수 N 에 대해서 트리 구조의 높이 h를 어느 정도로 하는가에 대해서는 많은 역할을 통합하여 트리 구조의 차수

가 큰 값을 갖도록 하고, 지나친 미세 역할 명세의 생성을 막아 전체 시스템이 적정한 복잡성을 가지도록 한다. 트리 구조의 차수에 따라 트리 구조의 높이가 정해지는데, 차수가 커지면 트리 구조의 높이가 낮아진다. 이는 통신 량을 줄이지만 단일 노드가 가져야 하는 역할 명세의 크기를 증가시킨다.

권한 구조 트리를 이루는 각 노드와 에지는 각각 컴퓨터와 통신 네트워크를 의미하며 이들은 실제 상황에서 완벽하게 동작하지 않는다. 각 노드는 장애의 가능성이 있으며, 사용자의 의도에 따라 각 노드가 예고 없이 제거되기도 한다. 그러므로 권한의 생성 시에는 노드의 신뢰도를 고려해서 하나 이상의 권한 정의 노드를 만들어 주거나 장애시점이 오기 전에 복제해야한다. 노드 간의 통신 네트워크도 불완전하여 항상 패킷손실의 가능성을 내포하고 있다. 그러므로 역할 명세 인증서 관리는 네트워크 고장률과 패킷 손실률을 보전하기 위해 데이터 복구, 패킷 재전송 등의 추가적인 비용이 요구된다. 다음 절에서 비용 분석을 위한 모델링을 한다.

3.2.1 노드 신뢰도 모델

네트워크 환경에서 컴퓨팅 노드의 존재는 시간에 따라 변화하여 고정되어 있지 않은데, 사용자 임의대로 생성되기도 하고 사라지기도 하며, 사용자의 의도와 상관없어 망가지기도 한다. 게다가 노드의 동작 여부에 대한 정보는 전파되는데 시간이 걸리므로 노드가 이루는 네트워크 환경에 대한 정확한 시각을 가지기는 어렵다. 그러므로 신뢰할 수 있는 노드 모델의 구성이 필요하다. 각 노드가 아무런 규제 없이 자유롭게 생성되고 제거되는 환경에서 각 노드는 무작위로 단조롭게(uniform)분포한다. 무작위 단조분포는 이항 분포(Binomial Distribution)로 표현된다. 노드의 생성은 비율 λ 의 포아송 프로세스(Poisson Process)를 따르는 것으로 가정한다. 포아송 분포는 이항 분포 B(k; p, n)에 $p=\lambda t/$, $q=1-p=1-\lambda t/n$을 대입한 후 $n\to\infty$ 을 취하여 얻는다. 노드의 삭제는 비율 μ을 가지는 지수분포(Exponential Distribution)를 따르는 것으로 가정한다[3]. 지수분포는 포아송 분포로부터 유추된다. 매개변수 μ의 지수분포에서 고장률(노드 삭제비율)이 μ이고, 평균 수명이 $1/\mu$ 이다. 시스템 내의 노드 수를 대략 일정하게 유지하기 위해 노드의 생성과 삭제가 같은 비율로 일어나는 포아송 프로세스임을 가정한다. 권한구조 트리에서 메시지가 전송될 때, 메시지가 장애노드로 전달될 확률은 지수분포의 성질에 따라 다음과 같이 구할 수 있다.

지수분포에서 확률 밀도 함수는 식 (1) 과 같고, 누적분포 함수는 식 (2) 와 같다.

$$f(t)=\mu e^{-\mu t},\ t\geq 0 \tag{1}$$

$$F(t)=\int_0^t f(x)dx=\int_0^t \mu e^{-\mu x}dx=1-e^{-\mu t} \tag{2}$$

식 (2)는 시간 t 안에 장애가 발생할 확률이다. 그러므로 메시지가 장애노드로 전달될 확률은 각 단계(hop)에서 식 (3)과 같다.

$$P_n=1-(1-e^{-r\mu})\cdot\frac{1}{\mu}\cdot\frac{1}{T} \tag{3}$$

식 (3) 에서 T는 장애를 감지하는데 드는 최대시간이다. 그러므로 메시지 손실률, L, 은 권한구조 트리에서 식 (4)과 같다.

$$L=1-(1-P_n)^l=1-\left(\frac{1-e^{-\mu T}}{\mu T}\right)^l \tag{4}$$

l 은 권한구조트리 내에서의 레벨간격으로 권한이 전달되는 단계(hop)수에 해당한다. 권한을 생성할 때는 $l=1$이 되어 메시지 손실률은 식 (5)와 같다.

$$L=1-\left(\frac{1-e^{-\mu T}}{\mu T}\right) \tag{5}$$

권한 명세를 적용할 때는 $l\geq 1$이므로 일반식 (4)로 계산된다.

노드 신뢰도는 응용 프로그램에 의해 증가될 수 있다. 응용 프로그램에서 메시지를 재전송할 수 있으며 플래그를 두어 각 노드마다 승인을 받도록 할 수도 있다. 이런 기법은 매우 높은 신뢰도를 보장한다. 이전에 선택된 노드가 장애상태일 경우 다른 노드를 선택할 수 있도록 하기 때문이다. 그러나 다음 노드가 고장인 것을 탐지하기위해 정해진 타임아웃시간동안 기다리는 것은 상당한 성능저하를 초래할 수 있다. 그러므로 메시지 손실률, L을 계산하고 그 값을 보전하도록 하여 성능과 신뢰도를 동시에 얻도록 한다. 타임아웃시간동안 기다리지 않고 효율적으로 메시지를 전송할 수 있는 확률을

높인다. 이를 감안하여 권한구조를 유지에 드는 비용을 구하기 위해서 비용 모델을 만들었다. 각 노드에서 발생되는 제어 트래픽은 노드 생성 및 변경에 따른 링크정보 테이블 갱신, 링크정보 테이블 유지관리 등 PMI 유지에 필요한 비용으로 다음과 같이 계산된다.

$$C = 1+L(1+L(1+L\cdots))\times 2\times(\lambda_c+\lambda_m)+N\times\frac{K}{T_k}$$
$$= \frac{2\cdot(\lambda_c+\lambda_m)}{1-L}+\frac{N\cdot K}{T_k} \quad (6)$$
$$= \frac{2\cdot(\lambda_c+\lambda_m)\cdot(\mu T)^l}{(1-e^{-\mu T})^l}+\frac{N\cdot K}{T_k}$$

첫 번째 항목에서 λ_c는 권한이 생성되는 사건의 발생 비율이고, λ_m는 권한이 갱신되는 사건의 발생 비율이다. 요청과 응답을 고려하여 2회의 패킷 전송을 계산하였다. $1/(1-L)$은 링크 정보 테이블 갱신에 따른 패킷전송량으로 손실률 L 을 보전한 것이다. 두 번째 항목은 링크정보 테이블의 엔트리 수, N에 대하여 K/T_k는 keep-alives등의 유지 관리 패킷 K를 송신간격 T_k로 나눈 값으로 초당 패킷수이다. 링크정보 테이블은 구조화되어 있지 않을 경우는 크기가 크지만 구조화 되어있는 경우는 테이블의 크기가 작으므로 유지관리 비용은 아주 적다.

3.2.2 통신 네트워크 신뢰도 모델

무선 망을 포함하여 신뢰도가 낮은 네트워크 상에서 규모 확장성을 제공하는 멀티캐스트 통신을 통하여 메시지를 전달한다. 그 기법은 다음과 같이 모델링 된다. 레벨 $l(0\le l\le h-1)$에서 메시지를 전송하고 할때, 모든 수신자 $R(l)$이 다 성공적으로 받을 때까지 메시지가 전송될 것이며, 그 전송횟수를 $M(l)$이라 하자. $R(l)$중의 하나의 수신자인 r이 메시지 k_i 를 전송받지 못할 패킷 손실률을 p라 하고, M_r은 r이 메시지 k_i를 성공적으로 받는데 필요한 패킷 전송횟수라 하자. 패킷 손실 사건(event)는 서로 독립적이므로, 메시지 전송횟수 M_r은 기하분포(Geometric Distribution)를 이루며 다음과 같이 계산된다.

$$P_e[M_r=m]=p^{m-1}(1-p) \quad (7)$$

$$P_e[M_r\le m]=1-p^m, m\ge 1 \quad (8)$$

식 (7)로부터

$$E(M_r)=\sum_{m=1}^{\infty} m\cdot P_e[M_r=m]$$
$$=1\cdot(1-p)+2\cdot(1-p)\cdot p+\cdots \quad (9)$$

(9)로부터 다음의 식을 얻을 수 있다.

$$E(M_r)=1/(1-p) \quad (10)$$

식(8)은 m번 이내에 성공적으로 메시지를 받을 확률이고, 식(10)는 평균 패킷 전송횟수이다. 각각의 수신자에게 발생하는 패킷 손실 이벤트가 서로 독립적이므로, 수신자 $R(l)$ 전부가 m 번 이내에 성공적으로 메시지를 받을 확률 $P_e[M(l)\le m]$은 식 (11)과 같다.

$$P_e[M(l)\le m]=\prod_{r=1}^{R(l)} P_e[M_r\le m]=(1-p^m)^{R(l)} \quad (11)$$

그러므로 평균 패킷 전송횟수는 식 (12)와 같이 계산된다.

$$E[M(l)]=\sum_{m=1}^{\infty} P_e[M(l)\ge m]=\sum_{m=1}^{\infty}(1-(1-p^{m-1})^{R(l)}) \quad (12)$$

이는 각각의 $R(l)$이 $m-1$번 이내의 패킷손실을 겪은 후 성공적 전송완료를 이루는 확률의 합이다. 장애 발생이 역할 명세 인증서의 관리에 주는 영향을 보면 네트워크 신뢰도 모델 하에서는 패킷 손실률 p에 비례해서 비용이 증가하고, 노드 신뢰도 모델 하에서는 노드 장애로 인한 수신자 $R(l)$의 변화에 따라 비용이 증가한다. $E[C_{PMI}]$을 역할 명세 인증서 관리에 드는 비용이라 하면 3.2.1과 3.2.2의 모델에서 $C_{PMI}=C\times R(l)$가 되므로 그 비용은 다음과 같다.

$$E[C_{PMI}]=\sum_{m=1}^{\infty}(1-(1-p^{m-1})^{C_{PMI}}) \quad (13)$$
$$C_{PMI}=C\times R(l)=\left(\frac{2\cdot(\lambda_c+\lambda_m)\cdot(\mu T)^l}{(1-e^{-\mu T})^l}+\frac{N\cdot K}{T_k}\right)\times R(l)$$

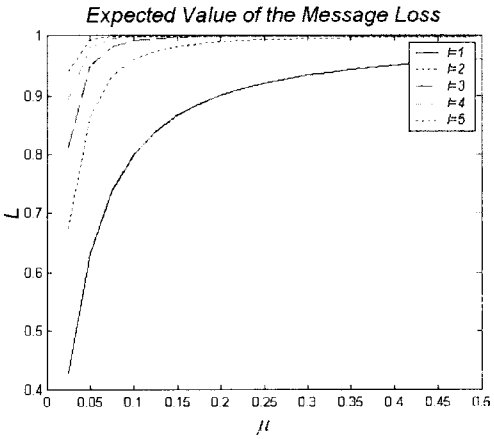
신뢰도를 나타내는 노드 고장률과 패킷 손실률에 따른 비용변화에 대한 분석은 4장에서 볼 수 있다.

Ⅳ. 성능 분석

4.1 메시지 손실률 분석

노드 장애로 인한 메시지 손실률 L과 권한 구조 유지

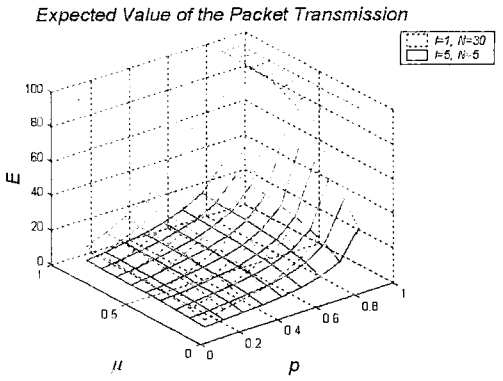
에 드는 비용 C를 식 (1)~(6)로부터 구하였다, 시스템 내의 노드 수를 대략 일정하게 유지하여 무한히 확장되거나 축소되는 네트워크를 가정하지 않기 위해 $\lambda_c = \mu$로 가정하였다. 편의상 λ_m도 같은 값으로 하였다. [그림 4]에서는 노드 고장률 μ에 따른 메시지 손실률 L을 나타내고 있다. 신뢰도가 낮은 네트워크에서 노드 고장률 μ는 더 큰 값을 가지게 되는데, μ가 커짐에 따라 메시지 손실이 급격히 증가함을 볼 수 있다. 또한 노드 고장률이 일정한 값일 경우, 역할 명세가 구조화되어 권한구조 트리내의 레벨 간격 l이 커지면 메시지 손실률 L이 증가함을 알 수 있다. 그러나 증가폭은 l의 증가율에 비해 점차 작은 값을 가진다.



〔그림 4〕 고장률에 따른 메시지 손실률

4.2 패킷 전송량 분석

식 (7)~(12) 로 계산된 네트워크 상의 패킷 손실률을 고려하여 식 (13)에 따라 평균 총 패킷 전송량 $E[C_{PMI}]$를 구하여 성능 비교 및 분석을 한다. 식 (12)에서 m 값이 10을 넘어가면 $E[C_{PMI}]$은 임계치에 근접하며 안정된 값을 가지므로, 충분히 큰 값으로, $m=100$을 주고 측정하였다. [그림 5]는 노드 고장률 μ와 패킷 손실률 p 값의 변화에 따른 평균 패킷 전송횟수 $E[C_{PMI}]$를 나타낸다. 신뢰도가 낮은 네트워크에서 μ와 p가 더 큰 값을 가지게 되므로 신뢰도의 감소에 따른 패킷 전송량의 증가를 그림에서 볼 수 있다. 권한 명세가 구조화되지 않은 경우는 $l=1$인 경우이고, 권한 명세가 구조화된 경우 $l<1$이므로 그림에서 $l=5$인 경우에 해당한다. 권한 구조 트리에서 차수 d가 2로 고정되어 있다면 권한 정



〔그림 5〕 고장률과 패킷 손실률에 따른 평균 패킷 전송량

보 테이블의 크기는 $N=2^l-1$이 된다. 차수는 2보다 클 수 있으므로 $N \geq 2^l-1$이다. 한정된 권한 명세에 대해서 차수 d가 커지면, 레벨 간격 l이 작아지고, 권한 정보 테이블의 크기 N은 커진다. 반대로 d가 작아지면, l이 커지고, N은 작아진다. [그림 4]에서 권한 명세가 구조화 되어 있는 경우에 l이 커지면서 메시지 손실률이 증가하는 것을 보았는데, 그럼에도 불구하고 [그림 5]에서 권한 명세가 구조화 되어 l이 커지는 경우에 N이 작아져서 평균 패킷 전송 횟수 $E[C_{PMI}]$가 크게 줄어들어 전체적으로 관리 비용의 이득을 얻는 것을 볼 수 있다.

4.3 트리 구조 분석

위의 실험에서 권한이 갱신되는 사건의 발생 비율 λ_m이 권한이 생성되는 사건의 발생 비율 λ_c의 2 배일 경우 즉, $\lambda_m = 2 \cdot \lambda_c$일 경우 패킷 전송 횟수 $E[C_{PMI}]$는 구조화되지 않은 경우에 12%, 구조화된 경우에 16% 증가되었다. 반대로 권한이 갱신되는 사건의 발생 비율이 절반일 경우 즉, $\lambda_m = 0.5 \cdot \lambda_c$일 경우 구조화되지 않은 경우 7%, 구조화된 경우 11% 감소되었다. 구조화된 경우 λ_m값의 변화에 따라 $E[C_{PMI}]$가 조금 더 영향을 받는 것을 볼 수 있다. 이는 권한 명세의 갱신이 아주 빈번할 경우 트리 구조의 차수를 늘려 레벨 간격 l을 줄여야 함을 의미한다. 레벨 간격 l을 줄인다는 것은 트리 구조의 높이를 낮춘다는 것인데, 극단적인 경우 구조화가 전혀 이루어지지 않게 된다 (l=1). 그러므로 권한이 갱신되는 사건의 발생이 빈번하지 않은 경우 캐시를 두는 것이 좋다 캐시로 쓸 수 있는 가용 메모리의 크기에 비례해서 트리 구조의 차수를 줄이고 레벨 간격을 늘리도록 하는 것이 실용적이라 하겠다. 실제 상황에서는

$\lambda_c > \lambda_m$인 경우가 많으므로 캐시를 크게 두어야하는 경우는 거의 발생하지 않는다.

기존 기법(l=1)과 비교하여 더 많은 성능향상을 얻으려면 l값을 보다 더 크게 하여야 한다. 예를 들어 p=0.3, μ=0.3인 경우, 평균 패킷 전송 횟수가 약 70 % 줄어든다. 이는 노드 장애가 빈번하고 패킷 전송이 신뢰할 수 없는 네트워크 환경에서 구조화되지 않은 권한 명세에 대한 모든 정보를 각 노드가 유지 관리하는 비용이 매우 큼을 보여주는 것이고, 상대적으로 구조화된 권한 명세가 더 적은 비용으로 효율적으로 운영될 수 있음을 나타내는 것이다. 그러나 한정된 역할 명세 내역에 따라 트리 구조의 높이는 제한되며, 응용에 따라서는 역할 명세의 변경이 적을 경우 권한을 사용하고자 할 때 역할 명세 인증서 체인을 따라가는 데 따른 성능 저하가 우세할 수 있으므로 적정한 차수로 역할 명세를 구조화하는 것이 바람직하다.

V. 결 론

오버레이 네트워크를 비롯한 고도의 동적인 협업 환경에서는 접근제어를 다양한 수준에서 제공해야 자연적인 동적변화에 적응하여 최적의 접근제어 기능을 제공할 수 있다. 이를 위해서는 기 성립된 접근제어 관계에서 얻을 수 있는 특성 및 신뢰관계를 잘 이용하는 것이 효율적이다. 본 논문은 고도로 분산된 환경에서, 신뢰도가 낮은 네트워크 환경에 적용할 유연한 구조의 권한 정의 모델을 찾고자 하는 노력의 결과이다. 역할 명세 인증서의 관계구조 트리를 구성하여 권한 정보를 트리 구조 내에서 주고받음으로써 안전하고 효율적인 권한의 관리를 달성한다. 권한 정보 전송을 위해 규모 확장성을 가지는 멀티캐스팅 패킷을 이용하며, 그에 따른 네트워크상의 패킷 손실률을 고려하였다. 또한 대규모 네트워크의 특징인 컴퓨팅 노드의 무작위 생성과 소멸을 고려하여 메시지 손실률을 구하였다. 노드의 생성 및 소멸, 패킷 손실률로 인한 신뢰도 저하를 고려하여 역할의 생성 및 갱신에 따른 비용구조를 모델링하고 성능을 측정, 분석하여, 역할 명세 인증서를 구조화하는 것이 메시지 손실률의 증가에도 불구하고 평균 패킷 전송량을 크게 줄여 전체적인 성능을 향상시킴을 정량적으로 보였다. 이는 유비쿼터스 환경이나 P2P 환경과 같은 신뢰도가 낮은 고도의 분산 컴퓨팅 환경에서 보다 적은 패킷 전송으로 신뢰성있는 권한 관리 구조를 만들 뿐 아니라 필요로 하는 데이터 전송에 드는 비용을 획기적으로 줄여 효율적인 접근 제어 및 권한 관리가 이뤄지도록 한다.

참고문헌

[1] S. Farrel and R. Hously "An Internet Attribute Certificate Profile for Authorization," IETF-RFC 3281, 2002.

[2] ITI, Role Based Access Control ITU/T. Recommendation X.509|ISO/IEC 9594-8, Information Technology Open Systems Interconnection - The Directory : Public-Key and Attribute Certificate Frameworks, 2003.

[3] C. English, P. Nixon, S. Terzis, A. McGetrtrick and H. Lowe, "Dynamic Trust Models for Ubiquitous Computing Environments," Workshop on Security in Ubiquitous Computing. 2002.

[4] D. Ferraiolo, R. Sandhu, S. Bavrila, D. Kuhn and R. Chandramouli, Proposed NIST Standard for Role-Based Access Control, ACM Transactions on Information and System Security, 4(3), 2001.

[5] J. Joshi, E. Bertino and A. Ghafoor, "Temporal hierarchies and inheritance semantics for GTR BAC," Proc. of the seventh ACM symposium on Access control models and technologies, pp.74-83, 2002.

[6] I. Djordjevic, T. Dimitrakos and D. Randal, "Dynamic Service Perimeters for Secure Collaborations in Grid-enabled Virtual Organizations : Overview of a proposed architecture," 2nd European Across Grids Conference, Jan. 2004.

[7] B. Lang et al, "Attribute Based Access Control for Grid Computing," Preprint ANL/MCS-P1367-0806, August 2006.

[8] Sandro Rafaeli, David Hutchison, "A Survey of Key Management for Secure Group Communication," ACM Computing Surveys, Vol. 35, No. 3, pp. 309-329, 2003.

[9] M. Castro, P. Druschel, A. -M. Kermarrec, A. Nandi, A. Rowstron and A. Singh, "Split Stream : High-Bandwidth Multicast in Cooperative

Environments," Proc. SOSP '03, Oct. 2003.

[10] D. Kostic, A. Rodriguez, J. Albrecht and A. Vahdat, "Bullet : High Bandwidth Data Dissemination Using An Overlay Mesh," ACM Symposium on Operating Systems Principles, 2003.

[11] C. Schlager, T.Nowey and J. Montenegro, "A Reference Model for Authentication and Authorisation Infrastructures Respecting Privacy and Flexibility in b2c eCommerce," Proc. of the First Int. Conf. on Availability, Reliability and Security (IEEE ARES '06), 2006.

[12] C. Schlager and N. Ganslmayer, "Effects of Architectural Decisions in Authentication and Authorisation Infrastructures," Proc. of the First Int. Conf. on Availability, Reliability and Security (IEEE ARES '07), 2007.

[13] KS X ISO/IEC 9594-8, 지식경제부 기술표준원, http://www.kats.go.kr

[14] ISO/IEC 9594-8, Information Technology Open Systems Interconn ection-The Directory : Public-Key and Attribute Certificate Frameworks, 2005.

[15] E. Palomar et al, "A. Ribagorda, Certificate-based Access Control in Pure P2P Networks," 6th IEEE International Conference on Peer-to-Peer Computing, 2006

〈著者紹介〉

양 수 미 (Soomi Yang) 정회원

1985년 2월 : 서울대학교 컴퓨터공학과 졸업
1987년 2월 : 서울대학교 컴퓨터공학과 석사
1997년 2월 : 서울대학교 컴퓨터공학과 박사
1988년 3월~2000년 9월 : 한국통신 연구소 연구원
2004년 9월~현재 : 수원대학교 인터넷정보공학과 교수
<관심분야> 정보보호, 시스템 보안, 네트워크 보안