역할 명세 인증서의 구조화에 의한 효율적 역할기반 접근제어 기법

An Efficient Role Based Access Control Technique by Structuring of Role Specification Certificate

양 수 미*
Yang, Soo mi

요 약

속성 인증서를 이용한 역할기반 접근제어를 함에 있어서 역할 관리 비용을 줄이기 위해 역할 할당 인증서와 역할 명세 인증서를 활용하면 역할의 변경에 따른 갱신 오버헤드를 줄일 수 있다. 특히 유비쿼터스 컴퓨팅 환경과 같은 고도의 분산 컴퓨팅 환경에서는 광범위한 통제 구조를 가질 수 없으므로 이를 고려한 속성 인증서 관리 기법이 요구된다. 역할 명세 인증서를 따로 두는 경우 역할 관리 비용이 줄어드는 바, 더 나은 성능향상을 위하여 본 논문에서는 역할 명세를 구조화하여 효율적 역할기반 접근제어를 위한 속성 인증서 관리 기법을 모색한다. 역할을 그룹화하여 역할 명세 인증서의 관계구조 트리를 구성하여 분산된 환경에서 안전하고 효율적인 역할의 갱신과 분배를 달성한다. 규모 확장성을 위해 멀티캐스팅 패킷을 사용한 역할 명세 인증서 분배를 하며, 그에 따른 네트워크 상의 패킷 손실율을 고려한 성능분석을 하여 역할 그룹을 두어 역할 명세 인증서를 구조화하는 것이 성능을 향상시킴을 정량적으로 보인다.

Abstract

In a role based access control through attribute certificate, the use of role assignment certificates and role specification certificates can reduce management cost and the overhead incurred by changing roles. Highly distributed computing environments such as ubiquitous computing environments not having global or broad control, need another attribute certificate management technique. Actually just having role specification certificate separately reduce management cost. But for better performance we structure role specification. We group roles and make the role group relation tree. It results secure and efficient role renewing and distribution. For scalable role specification certificate distribution, the multicasting of packets is used. We take into account the packet loss and quantify performance enhancements of structuring role specification certificates.

☞ Keyword : role based access control, attribute certificate, privilege management infrastructure(PMI)

1. 서 론

ANSI/INCITS (American National Standards Institute/International Committee for Information Technology Standard) 에서는 2004년도에 ANSI INCITS 359-2004 [3,4]에서 역할기반 접근제어(RBAC, Role Based Access Control)를 정보 기술 산업 표준으로 하였다. 이는 역할기반 접근제어가 정보산업의 기반이며 매우 중요함을 나타낸다. 유연한 동적구조를 가지는 고도의 분산화된 네트워크 기반의 다양한 응용이 증가하면서 그룹화되고 협동적인 응용이 일반화되고 있으므로 역할기반 접근제어도 그러한 네트워크 환경을 고려해서 정의되어야 한다. 유비쿼터스 컴퓨팅 환경과 같은 고도의 분산화된 네트워크를 포함하는 자율적이면서 유연한 협업 환경을 고려해야한다. 이에 주체 및 객체와 그 관계를 모델링함에 있어서 위의 표준을 수용하면서 이를 확장하는 보안 모델이 요구된다.

* 정 회 원 : 수원대학교 인터넷정보공학과 교수
smyang@suwon.ac.kr(제1저자)
[2005/03/10 투고 - 2005/03/29 심사 - 2005/04/25 2차 심사 - 2005/04/27 심사완료]

근래의 고도의 네트워크 환경으로 대두되고 있는 유비쿼터스 컴퓨팅 환경은 대량의 네트워크로 연결된 무선 기기가 중앙의 제어 없이 자율적으로 상호작용하는 동적 환경으로 대표된다. 중앙의 통제가 없을뿐 아니라, 응용이 완결되지 않은 채 접속이 종료되는 객체들로 인하여 전체적으로 정리된 관리 구조가 유지되지도 않는다. 우리는 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 하는 경우, 오픈된 네트워크가 가지는 보안상의 문제점을 가지게 된다. 그러한 오픈된 네트워크 환경에서 보안을 고려하기 위해서는 중앙의 통제 없이 사용자의 인증과 접근제어를 이룰 수 있어야 한다. 현존하는 보안 기반구조가 이러한 증가하는 유연성에 적합하지 않으므로, 이를 위해 인증과 접근제어에 있어서 분산된 신뢰 구조(trust structure)가 제안되었다[11,12]. 신뢰 구조에서는 역할기반 접근 제어를 하며 권한 위임 기법을 쓴다. 본 논문에서는 신뢰구조의 철학을 접근제어를 위한 속성 인증서 관리에 적용, 역할 명세 인증서 간의 신뢰구조를 확립한다. 이것은 신뢰 구조가 가지는 권한 위임과는 다르며, 권한의 분산으로 생각할 수 있다. 역할을 그룹화하여 새로이 역할그룹을 정의하며, 이는 객체를 그룹화하여 역할을 할당하는 기존의 일반적 역할 인증서 사용 방법과는 다른 방식이다.

멀티캐스트는 그룹 통신을 위한 효율적이고 규모 확장성을 가진 기술로 각광받고 있다. 본 논문에서는 역할 그룹의 역할 명세 인증서의 분배에 적용하여 효율성을 제공한다.

논문의 순서는 다음과 같다. 2장에서 역할 그룹 모델을 설계하고 역할 그룹화를 정의한다. 3장에서 역할 갱신 통신 모델을 정의하고 분석한다. 4장에서 성능 분석 결과를 보이고, 5장에서 관련 연구에 대한 소개를 하고, 6장에서 요약과 함께 결론을 맺는다.

2. 역할 그룹 모델

역할 그룹은 (G, K, R) 삼원식으로 표현된다. G는 유한하고 비어있지 않은 역할그룹($Group_i$)의 집합이다. $Group_i$는 유한하고 비어있지 않은 역할(r_i)의 집합이다. K는 유한하고 비어있지 않은 키의 집합으로 그룹 키(TEK_i, Traffic Encryption Key)를 포함한다. R은 G와 K사이의 이원관계로 안전한 그룹 통신에 관여되는 역할 그룹과 그룹 키 사이의 관계를 나타낸다. 그러므로 $R_i \subset G_i \times K_i$가 된다. 그룹 키는 안전한 역할 그룹을 이루는 역할의 집합에 대한 키 서버 KS_i가 키 생성과 분배를 책임진다. KS_i가 생성하는 키는 K에 속한 TEK_i에 해당한다. 키 서버는 역할 그룹과 그룹 키 간의 관계 R_i

version (인증서버전)
holder(속성인증서소유자)
issuer(인증서발급자)
signature(서명)
serialNumber(순서번호)
attrCertValidityPeriod(유효기간)
attributes(속성)
issuerUniqueID(발급자ID)
extensions(확장)

〈그림 1〉 속성 인증서의 형식

version (인증서버전)
serialNumber(순서번호)
signature(서명)
issuer(인증서발급자)
validity(유효기간)
subject(공개키주체)
subjectPublicKeyInfo(공개키정보)
issuerUniqueIdentifier(발급자ID)
extensions(확장)

〈그림 2〉 공개키 인증서의 형식

holder	attributes	extensions

〈그림 3〉 간략화된 속성 인증서의 형식

subject	publicKeyInfo	extensions

〈그림 4〉 간략화된 공개키 인증서의 형식

에 대한 정보를 유지한다. 그룹간의 트리 관계에 따라 그룹 키도 트리를 구성하게 된다.

[4,5] 의 표준에 정의된 속성 인증서의 형식은 그림 1과 같고 대비되는 공개키 인증서의 형식은 그림 2와 같다. 각 필드에 대한 설명은 [4,5]를 참고하기 바란다.

그림 1에서 본 논문에서 다루는 필드는 holder, attributes, extensions로, 각각 속성인증서의 소유자, 속성, 확장 필드를 나타낸다. 속성은 일반적으로 역할을 가리키며, 확장 필드는 용도가 개방되어 있다. 이들은 공개키 인증서의 subject(공개키 인증서의 주체), subjectPublicKeyInfo(주체의 공개키 정보), extensions(확장) 필드에 해당한다. 이 필드들만으로 이루어진 간략한 형식으로 나타내면 각기 그림 3, 4와 같다. 이를 이용하여 간략한 표현을 들어 논문의 내용을 설명하고자 한다.

속성인증서의 소유자(holder)에는 공개키 인증서의 주체(subject)에 해당하는 사용자 혹은 역할이름이 올 수 있다. 또한 속성(attributes) 필드에는 역할(role)을 비롯하여 access identity, group, clearance, audit identity, charging identity 등이 올 수 있으며, 경우에 따라 비어있을 수도 있다. 확장(extensions) 필드는 필요에 따라 자유롭게 정의될 수 있어, 속성인증서의 활용도를 높인다.

[4,5]에 정의된 권한 관리 구조(PMI, Privilege Management Infrastructure)의 역할 모델에서 속성 인증서는 역할을 소유자(주체)에게 할당하는 역할 할당 인증서(Role Assignment Certificate)와 정의된 역할에 대한 명세를 가지는 역할 명세 인증서(Role Specification Certificate)로 구분된다. 역할 할당을 변경하지 않고 역할에 대한 명세만을 독립적으로 바꿀 수 있도록 하기 위함이다. 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 identifier를 가진다. 역할 명세 인증서의 소유자(holder)는 역할 할당 인증서의 역할명(roleName)에 해당한다. 본 논문에서는 역할 명세 인증서의 역할 확장 필드가 다른 역할 명세 인증서의 정보(예를 들어 identifier, 역할 명세 인증서의 순서번호)를 가지도록 하여, 역할 명세를 구조화한다. 또한 구조화를 돕기 위해 역할을 그룹화한다.

역할 그룹을 두는 경우 권한을 사용하고자 할 때 역할 명세 인증서의 체인을 따라가야 하는 경우 성능저하가 있을 수 있다. 그러므로 역할 명세 인증서를 캐쉬하여 효율적 사용이 가능하도록 한다. 효율적 캐싱의 방법은 [6]에 제시되어 있고 [10]을 참고할 수 있으며, 본 논문에서는 역할 할당에 변화가 있어 역할 명세 인증서를 갱신해야할 경우에 대해서 논한다.

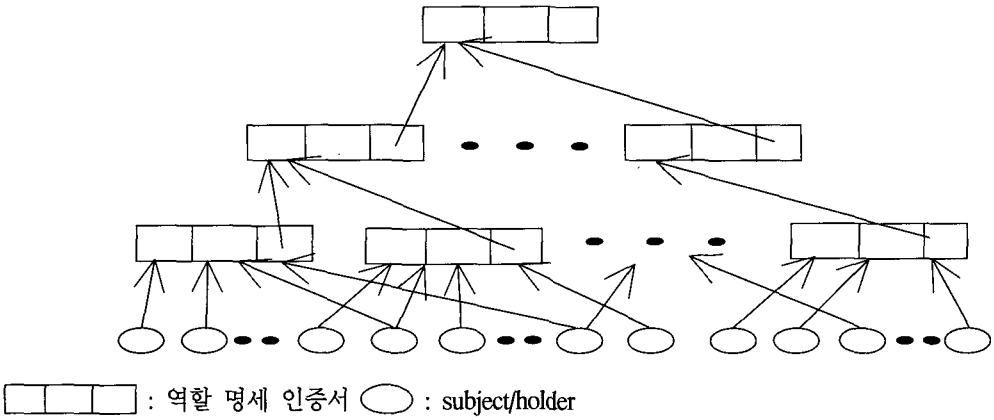
역할 할당 인증서로 속성 인증서 혹은 공개키 인증서를 이용할 수 있다. 공개키 인증서를 사용할 경우, 확장필드에 역할 명세 인증서에 관한 정보를 가지게 된다. 반면에 역할 할당 인증서로 속성 인증서를 사용할 경우, 그림 5과 같은 내용을 속성 인증서가 가지게 된다.

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

〈그림 5〉 역할 할당 인증서의 내용

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

〈그림 6〉 역할 명세 인증서의 내용



〈그림 7〉 역할 명세 인증서의 그룹 구조화

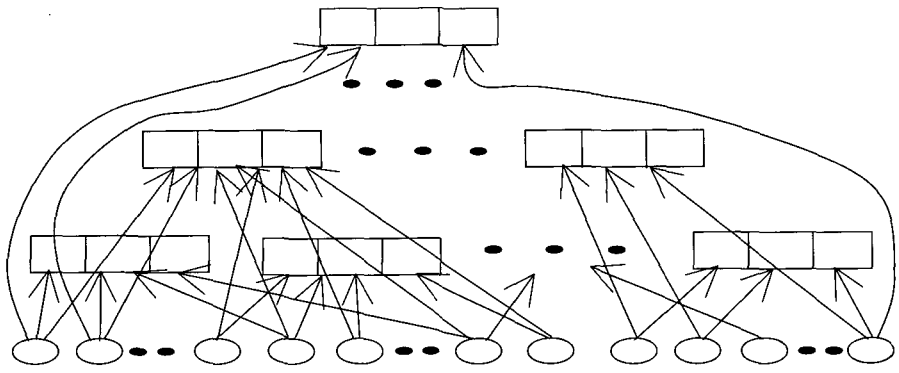
즉, 소유자(holder) 필드에 pkc(public key certificate, 공개키 인증서) subject를, 속성(attributes) 필드에 역할을, 확장(extensions) 필드에 역할 명세서 인증서에 대한 링크를 가진다. 그에 따른 역할 명세 인증서의 형식은 그림 6과 같다.

확장(extensions) 필드에 다른 역할 명세 인증서 정보-역할 이름(roleName) 또는 역할 명세서 순서번호(serialNumber)-을 넣어 그림 7과 같이 나무 구조를 이룬다.

새로 상위 노드에 명세가 정의되는 역할을 역할 그룹으로 명명한다. 표준[4,5]에서는 기술적으로 이러한 구조가 가능하도록 정의되어있으나 역할 적용시의 오버헤드로 이용이 제한되고 있다. 그러나 각 노드가 네트워크를 통해 고도로 분산되어 있는 경우 역할 적용시의 오버헤드에 비해 역할 갱신시에 얻는 성능 상의 이익이 더 크다. 역할 적용시의 오버헤드는 캐싱으로 극복할 수 있으므로, 역할 갱신시의 오버헤드를 줄이면 이는 고도의 분산된, 신뢰성이 낮은 네트워크 환경에서 매우 효과적이다. 이것을 정량적으로 보이는 것이 본 논문의 목적이라고 하겠다.

역할 그룹을 사용하지 않을 경우 역할 소유자(holder)가 모든 역할 명세 인증서를 가져야 하며, 그림 8과 같이 표현된다.

그림 8의 경우, 역할의 적용이 하나의 단계로 이루어지는 장점이 있으나, 저장해야하는 역할 명세 인증서 크기가 늘어나며, 소규모 메모리를 가지는 유비쿼터스 환경의 무선 단말의 경우 사용에 제약을 받게 된다.



〈그림 8〉 역할 명세 인증서의 비그룹 구조화

3. 역할 갱신 통신 모델

그림 7과 같이 역할 명세 인증서가 체인을 이룰 경우, 역할의 적용에 있어서 추가의 시간이 소요된다. 이를 개선하기 위하여 역할 명세 인증서에 대하여 응집성 캐싱을 한다. 응집성 캐싱을 위하여 통신 패턴이 그룹 내에서 분석되며 응집성의 정도에 따라 캐싱의 정도가 결정된다. 응집성이 높을수록 캐싱의 확률이 높다. 효율적 캐싱의 방법 및 성능 분석은 [6,10]에 제시되어 있다. 본 논문에서는 역할의 갱신에 따른 역할 명세서 정보 갱신에 초점을 맞춘다.

갱신된 역할 명세 인증서는 규모 확장성을 제공하는 멀티캐스트 통신을 통하여 전달되며, 그 기법은 다음과 같이 모델링된다.

R : 역할 (r_i)의 수

N : 최하위 역할 그룹의 최대 개수,

$\binom{R}{1}+\binom{R}{2}+\binom{R}{3}+\ldots+\binom{R}{R-1}+\binom{R}{R}$ $\binom{R}{1}$은 역할을 한 개 가지는 역할 그룹이고, $\binom{R}{R}$은 모든 역할을 포함하는 역할 그룹으로 transitive한 경우이외에 실질적 의미는 거의 없으나 완전성을 갖추기 위하여 포함한다.

k : 최하위 역할 그룹 명세 인증서의 최대 개수 $=N$

n_i : 역할 그룹 i (i번째 역할 그룹)

k_i : 역할 그룹 n_i에 관련된 역할 그룹 명세 인증서

h : 트리의 높이 (루트의 레벨은 0이고 단말의 레벨은 $h-1$이다.)

d_i : 역할 그룹 n_i의 차수

이해를 돕기 위해 그림 7의 그래프 구조를 점선 부분이 없는 것으로 가정하고 각 변수의 값을 알아보면, R은 최하위에 있는 역할 명세 인증서의 개수에 해당하고, $N=\binom{3}{1}+\binom{3}{2}+\binom{3}{3}$이므로, $R=3$, $N=7, k=7$이다. 그래프에서 실제로 구성된 역할 그룹은 3개이고, 각각 하위 노드가 2, 2, 1개이므로, $n_i=\{n_1,n_2,n_3\}, k_i=\{k_1,k_2,k_3\}, h=3, d_i=\{d_1=2, d_2=2, d_3=1\}$이다. 모든 중간노드의 차수를 $d_i=d$ (예를 들어 2)로 하면, $N=d^{h-1}$ (예를 들어 4)가 된다.

N에 대해서 h를 어느 정도로 하는 것이 좋은가에 대해 알아보기 위해 다음 표 1에 보인 바와 같이 R에 따른 $N=\binom{R}{20}$의 값을 계산하였다. 이것으로 $N'(>>N)$이 아주 큰 값을 가지게 되리라는 것을 알 수 있다. 그러므로 많은 역할을 그룹화하여 나무구조의 차수가 큰 값을 갖도록 하고, 지나친 그룹의 생성을 막아 전체 시스템이 적정한 복잡성을 가지도록 한다. 나무구조의 차수에 따라 나무구조의 높이가 정해지며, 이에 대한 분석은 4장에서 보인다.

레벨 l ($0 \le l \le h-1$)에서 역할 그룹 n_i의 역할 명세 인증서 k_i의 갱신이 있다고 하자. 그러면 역할이 그룹화되어 있지 않는 경우, 역할 명세 인증서는 전체 subject/holder의 수만큼 정보갱신이 필요하며 각각은 d^{h-l} 역할 관리자에게 전송되어야 한다. 즉 역할 명세 인증서의 수신자 $R(l)=d^{h-l}$이다. 반면에 역할이 그룹화되어 있는 경우, 명세 인증서는 하위 역할 그룹의 수만큼의 정보갱신이 필요하며 각각은 d 역할 관리자에게 전송되어야한다. 즉 역할 명세 인증서의 수신자 $R(l)=d$ 이다.

레벨 l의 역할 명세 인증서가 갱신되었다고 하자. 모든 $R(l)$이 다 성공적으로 받을 때까지 역할 명세 인증서가 전송될 것이며, 그 전송횟수를 $M(l)$이라 하자. $R(l)$중의 하나의 수신자인 r이 k_i를 전송받지 못할 패킷 손실율을 p라 하고, M_r은 r이 키 k_i를 성공적으로 받는데 필요한 역할 명세 패킷 전송횟수라 하자. 패킷 손실 사건(event)는 서로 독립적이므로, 역할 명세 전송횟수 M_r은 기하분포(Geometric Distribution)를 이루며 다음과 같이 계산된다.

〈표 1〉 R에 따른 N 값의 변화

R	100	500	1000	5000	10000
N'	5.36E+20	2.67E+35	3.39E+41	3.77E+55	4.03E+61

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

$$P[M_r \le m] = 1 - p^m, m \ge 1 \quad (2)$$

식 (1)로부터

$$E(M_r) = \sum_{m=1}^{\infty} m \cdot P[M_r = m] = 1 \cdot (1-p) + 2 \cdot (1-p) \cdot p + \cdots \quad (3)$$

$$p \cdot E(M_r) = 1 \cdot (1-p) \cdot p + 2 \cdot (1-p) \cdot p^2 + \cdots \quad (4)$$

(3)-(4) 로부터 다음의 식을 얻을 수 있다.

$$(1-p) \cdot E(M_r) = (1-p)[1 + p + p^2 + \cdots] = (1-p) \cdot (\frac{1}{1-p}) = 1 \quad (5)$$

$$E(M_r) = 1/(1-p) \quad (6)^{1)}$$

식 (1)은 m번 이내에 성공적으로 역할 명세 인증서를 받을 확률이고, 식 (6)는 평균 역할 명세 인증서(패킷) 전송횟수이다. 각각의 수신자에게 발생하는 패킷 손실 이벤트가 서로 독립적이므로, 수신자 $R(l)$ 전부가 m번 이내에 성공적으로 키를 받을 확률 $P[M(l) \le m]$은 식 (7)과 같다.

$$P[M(l) \le m] = \prod_{r=1}^{R(l)} P[M_r \le m] = (1-p^m)^{R(l)} \quad (7)$$

그러므로 평균 역할 명세 패킷 전송횟수는 식 (8)와 같이 계산된다.

$$E[M(l)] = \sum_{m=1}^{\infty} P[M(l) \ge m] = \sum_{m=1}^{\infty} (1 - (1-p^{m-1})^{R(l)}) \quad (8)$$

즉, 각각의 $R(l)$이 $m-1$번 이내의 패킷손실을 겪은 후 성공적 전송완료를 이루는 확률의 합이다.

1) 이 평균값은 다음과 같이 구해도 된다.

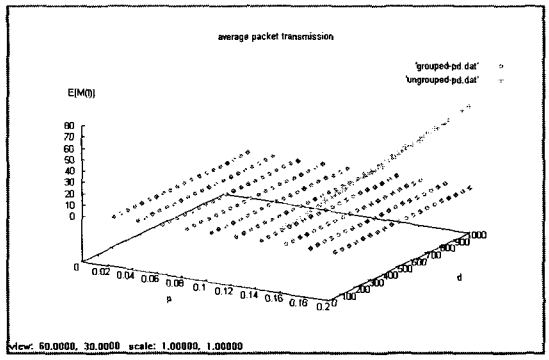
$$E[M_r] = \sum_{m=1}^{\infty} P[M_r \ge m] = \sum_{m=1}^{\infty} 1 - (1-p^m) + p^{m-1} \cdot (1-p)$$

$$\sum_{m=1}^{\infty} p^{m-1} = 1/(1-p)$$

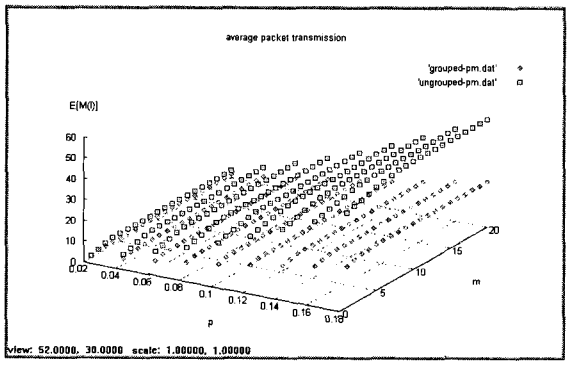
4. 성능 분석

식 (1)~(4)로부터 평균 역할 명세 패킷 전송 회수 $E[M(l)]$ 을 구하여 성능 비교 및 분석을 한다. 먼저 패킷 손실율 p 값에 대하여, 역할 명세 나무 구조의 차수의 변화가 평균 역할 명세 패킷 전송 횟수에 미치는 영향을 살펴보았다. 그림 9를 보면 패킷 손실율이 작을 경우 역할이 그룹화되어 있는 경우(grouped-pd.dat)와 역할 그룹화되지 않은 경우(ungrouped-pd.dat)의 차이가 별로 없지만, 패킷 손실율이 커짐에 따라 역할이 그룹화되지 않은 경우 평균 역할 명세 패킷 전송횟수가 급격히 늘어남을 볼수 있다. 그리고 d가 커짐에 따라 그 차이가 더욱 커지므로 그룹화하는 경우에 성능상의 이익이 더욱 커진다. 그러나 극단적인 성능의 차이를 돋보이고자하는 것이 본 논문의 목적이 아니므로 이하의 분석에서는 $d = 50$을 가정하여 적절한 수준에서의 성능 비교를 수행한다.

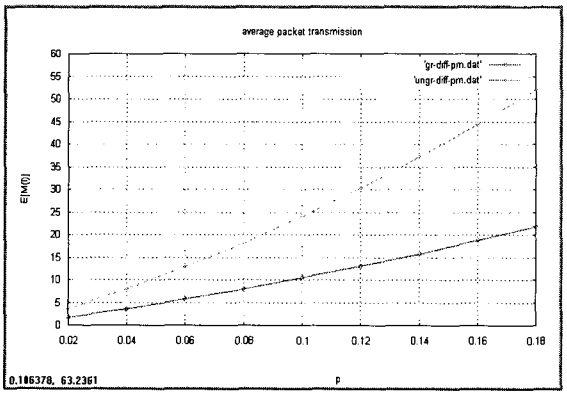
그림 10는 패킷 손실율 p와 임계치(threshold) m값의 변화에 따른 평균 패킷 전송횟수 $E[M(l)]$를 나타낸다. m 값이 10을 넘어가면 $E[M(l)]$은 임계치에 근접하며 안정된 값을 가진다. $m = 20$일 경우, p 값의 변화에 따른 $E[M(l)]$의 값을 비교하면 그림 11과 같다. 그룹화되지 않았을 경우(ungrouped-pm.dat) 평균 (역할 명세) 패킷 전송횟수 $E[M(l)]$이 급격히 커지나, 그룹화되었을 경



〈그림 9〉 p와 d의 변화에 따른 평균 역할 명세 패킷 전송횟수



〈그림 10〉 p와 m의 값의 변화에 따른 평균 역할 명세 패킷 전송횟수



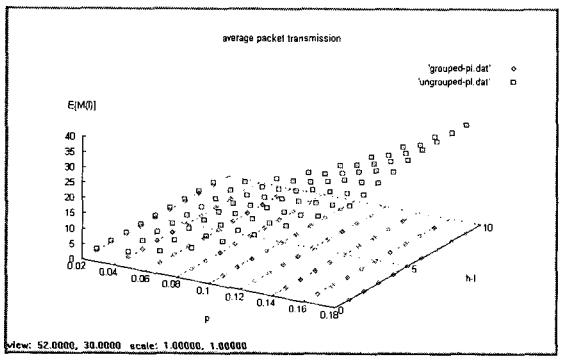
〈그림 11〉 $m=20$ 인 경우 평균 역할 명세 패킷 전송횟수

우(grouped-pm.dat) 완만한 증가를 보인다. 즉, $p=0.1$인 경우 50%, $p=0.16$인 경우 40% 정도로 평균 패킷 전송횟수가 줄어드는 성능 향상을 볼 수 있다.

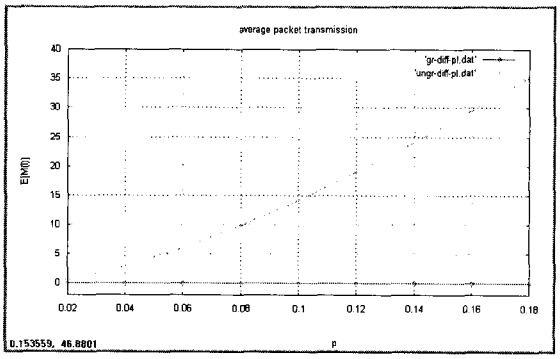
그림 12는 패킷 손실율 p와 전체 나무 구조 내에서 역할 명세 인증서 갱신이 발생한 레벨의 레벨 차이$(h-l)$에 따른 평균 역할 명세 패킷 전송횟수를 나타낸다. 비교를 쉽게 볼 수 있도록 하기 위해 레벨차이가 5일 경우에 대해 이차원 그래프를 그린 것이 그림 13이다. 그룹화되지 않았을 경우(ungrouped-pl.dat) 평균 패킷 전송횟수 $E[M(l)]$이 급격히 상승하나 그룹화 되어있을 경우(grouped-pl.dat) 평균 패킷 전송횟수가 현저히 낮을 뿐 아니라 패킷 전송횟수 증가의 변화가 미소함을 볼 수 있다. 그래서 $p=0.02$일 경우 40%, $p=0.1$일 경우 30%, $p=0.18$일 경우 26% 정도로 패킷 전송횟수가 점진적으로 줄어들어 네트워크 환경이 열악해 질수록(p가 커질수록) 성능상의 이익이 커짐을 알 수 있다.

5. 관련 연구

R. Sandu [1]와 D. Ferraiolo [2] 는 NIST의 표준[3]을 제안한 대표적인 역할기반 접근제어 연구자이다. R. Sandu는 [1]에서 역할기반 접근제어를 사용자, 역할, 관리자 등의 요소를 조합하는 역



〈그림 12〉 p와 l의 변화에 따른 평균 역할 명세 패킷 전송횟수



〈그림 13〉 $(h-l)=5$일 경우 평균 역할 명세 패킷 전송횟수

할기반 접근 제어를 모델링하고, 역할의 생성, 권한 할당, 권한 제거, 역할의 제거에 이르기까지 사용 예를 설명하여, 향후 다양하게 발전하는 역할기반 접근제어의 초석을 놓았다. D. Ferraiolo,는 [2]에서 역할의 우선순위 관계를 설명하고 이를 구현한 예를 보였다. 이후 이들의 연구에 뒤이은 여러 종류의 역할기반 접근제어 기법이 제시되었으나 사용자(주체)의 그룹에 대한 역할만 다루고 있으며 역할의 그룹화에 대한 논의는 없다. 그래도 본 연구와 관련이 될만한 것을 꼽는다면 J. Joshi의 시간개념을 추가한 위임 관계모델이다[9]. [9]에서는 시간에 따라 변화하는 동적 환경을 대상으로 권한 위임의 유연성을 제고하였다. 그러나 본 논문에서 제시하는 역할의 그룹화나 멀티캐스팅의 개념은 고려되지 않았다.

멀티캐스팅은 [7]에서 제안된 표준에 따라 실현되며, 멀티캐스팅을 이용한 다양한 키의 전달 방식은 [8]에 소개되어있다. [8]에서는 키의 전달에 초점을 맞추고 있으며, 본 논문의 역할 명세 인증서의 전달은 [8]의 응용선상에 있다고 하겠다.

6. 결 론

보안이 요구되는 협업 환경에서 접근제어를 다양한 수준에서 제공해야 자연적인 동적변화에 적응하여 최적의 접근제어 기능을 제공할 수 있다. 이를 위해서 기 성립된 접근제어 관계에서 얻을 수 있는 특성 및 신뢰관계를 이용하는 것이 효율적이다. 이에 개별 역할에서 공통된 부분을 그룹화하고, 역할 그룹의 역할 명세 인증서의 관계구조 트리를 구성하여 분산된 환경에서 안전하고 효율적인 역할의 갱신과 분배를 달성한다.

규모 확장성을 위해 멀티캐스팅 패킷을 이용한 역할 명세 인증서 분배를 하며, 그에 따른 네트워크 상의 패킷 손실율을 고려한 성능분석을 하였다. 역할 그룹을 두어 역할 명세 인증서를 구조화하는 것이 역할의 갱신시에 발생하는 패킷 전송횟수를 크게 줄여 성능을 향상시킴을 정량적으로 보였다.

참 고 문 헌

[1] R. Sandhu, V. Bhamidipati and Q. Munawer, The ARBAC97 Model for Role-based Administration of Roles, ACM Transactions on Information and System Security. Vol.2, No.1, pp.105-135, 1999

[2] David Ferraiolo, John F. Barkley and D. Richard Kuhn, "A Role-Based Access Control Model and Reference Implementation Within a Corporate Intranet", ACM Transactions on Information and System Security, Vol. 2, No. 1, pp. 34-64, 1999

[3] D. Ferraiolo, R. Sandhu, S. Bavrila, D. R. Kuhn and R. Chandramouli, Proposed NIST Standard for Role-Based Access Control, ACM Transactions on Information and System Security, 4(3), pp. 224-274, 2001

[4] ITI (Information Technology Industry Council), Role Based Access Control ITU/T(2001). Recommendation X.509 | ISO/IEC 9594-8, Information Technology Open *Systems Interconnection - The Directory*: Public-Key and Attribute Certificate Frameworks, 2003

[5] S. Farrell and R. Housley, An Internet Attribute Certificate Profile for Authorization, IETF RFC 3281, 2002

[6] 양수미, "그룹 키를 이용하는 응집성 권한 위임 캐쉬을 제공하는 역할기반 접근 제어", 수원대학교 논문지, 2004.

[7] H. Harney, U. Meth, A Colegrove and G. Gross, "GSAKMP", internet-draft : draft-ietf-msec-gsakmp-sec-06.txt, 2004.

[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] James B D Joshi, Elisa Bertino, Arif Ghafoor, "Temporal hierarchies and inheritance semantics for GTRBAC", Proceedings of the seventh ACM symposium on Access control models and technologies, Monterey, California, USA, pp.74-83, 2002

[10] Arthur Goldberg, Robert Buff, Andrew Schmitt, "Secure Web Server Performance Dramatically Improved by Caching SSL Session Keys", Workshop on Internet Server Performance, 1998

[11] Colin English, Paddy Nixon, Sotirios Terzis, Andrew McGetrtrick and Helen Lowe, "Dynamic Trust Models for Ubiquitous Computing Environments", Workshop on Security in Ubiquitous Computing (UBICOMP), 2002

[12] Lalana Kagal, Tim Finin and Anupam Joshi, "Moving from Security to Distributed Trust in Ubiquitous Computing Environments", IEEE Computer, 2001

◐ 저 자 소 개 ◑

양 수 미 (Yang, Soomi)
1985년 서울대학교 컴퓨터공학과 졸업(학사)
1987년 서울대학교 대학원 컴퓨터공학과 졸업(석사)
1997년 서울대학교 대학원 컴퓨터공학과 졸업(박사)
2004년 ~ 현재 수원대학교 인터넷정보공학과 교수
관심분야 : 정보보호
E-mail : smyang@suwon.ac.kr