Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1025

소셜 네트워크 환경에서 동적 신뢰 중심의 접근 제어 모델에 관한 연구*

백 승 수,[1,2†] 김 승 주[2‡]
[1]육군사관학교 전자정보학과, [2]고려대학교 정보보호대학원

Study on Dynamic Trust-based Access Control in Online Social Network Environment*

Seungsoo Baek,[1,2†] Seungjoo Kim[2‡]
[1]Department of Electronic Engineering & Information Science, Korea Military Academy
[2]CIST(Center for Information Security Technologies), Korea University

요 약

최근 10여 년간 온라인 소셜 네트워크(Online Social Network, OSN)의 사용인구가 폭발적으로 증가하고 있고 우리 생활에서 빼 놓을 수 없는 요소가 되었다. OSN은 개인뿐만 아니라, 그룹, 조직, 그리고 지정학적 위치, 시간적 제약조건까지 극복하는 시공을 초월한 사회적 관계의 확장을 가져오고 있다. 이러한 관계 및 정보공유의 확장은 사생활 노출, 무분별한 정보 공유, 거짓 정보의 전파 등 많은 부작용을 낳기도 한다. 이러한 부작용을 통제하기 위해 MAC, DAC, RBAC 등 기존의 접근제어 방법이 사용되었으나, 사용자 간의 접근 허용의 범위가 고정되어, 지속되는 관계 변경에 따른 접근 범위의 제한이 어렵고, 그러므로 변화하는 사용자의 악의적인 행동에 대한 대책이 미흡하다. 본 논문에서는 OSN 환경에 맞는 사용자간 동적 신뢰 중심의 접근제어 모델을 제안하여 사용자의 신뢰도의 변화에 따라 접근 권한을 변화시켜 사용자의 악의적인 행동 변화를 제어토록 하겠다.

ABSTRACT

There has been an explosive increase in the population of OSN(online social network) for 10 years. OSN provides users with many opportunities to have communication among friends, families and goes so far as to make relationships among unknown people having similar belief or interest. However, OSN also produced adverse effects such as privacy breaches, leaking uncontrolled information or disseminating false information. Access control models such as MAC, DAC, RBAC are applied to the OSN to control those problems but those models in OSN are not fit in dynamic OSN environment because user's acts in OSN are unpredictable and static access control imposes burden on users to change access control rules one by one. This paper proposes the dynamic trust-based access control to solve the problems of traditional static access control in OSN.

Keywords: Online Social Network, Dynamic Trust, Access Control, Trust Evaluation

접수일(2013년 9월 12일), 수정일(2013년 10월 11일), 게재확정일(2013년 10월 11일)
* 본 연구는 미래부가 지원한 2013년 정보통신·방송(ICT) 연구개발사업의 연구결과로 수행되었음.

† 주저자, baek.seungsoo@gmail.com
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

I. 서 론

최근 10여 년간 Facebook, MySpace, Google+ 등 OSN(이하, Online Social Network)의 사용 인구가 폭발적으로 증가하고 있고, 우리 생활에서 빼놓을 수 없는 요소가 되었다. OSN의 사용자 중심, 관계 중심, 자유로운 정보생산 및 이동, 정보에 대한 피드백 등의 대표적인 특징을 이용하여 우리는 기존 오프라인 친구, 동료, 가족이 온라인상에서 서로 의사소통을 하기도 하고, 자신의 신념이나 관심사가 비슷한, 오프라인에서는 서로 알지 못했던 사람과도 관계를 맺고 정보공유를 한다. 이러한 OSN의 특징을 통해 개인뿐만 아니라, 그룹, 조직, 그리고 지정학적 위치, 시간적 제약조건까지 극복하는 시공을 초월한 사회적 관계의 확장을 가져오고 있다.

하지만 이러한 관계 및 정보공유의 확장은 사생활 노출, 무분별한 정보 공유, 거짓 정보의 전파 등 많은 부작용을 낳기도 한다. 또한, 정보의 홍수 속에서 미확인 정보의 유통이 많아지면서 개인 정보와 아이디어 내용 그 자체의 중요성을 강조하는 것이 아닌 그 정보를 제공하는 사람 또는 내 정보에 접근 하는 사용자가 얼마나 믿을 만한가, 즉 정보 공유를 위해 사용자의 신뢰가 중요한 관심사가 되고 있다. 이러한 기능은 기존은 보안에서 강조되어 왔던 무결성, 인증, 부인방지 기술과 같은 정보 그 자체를 보호하는 것으로는 방지하기 힘들다.

OSN에서 사용자의 신뢰를 판단하기 위해서 우리는 다음과 같은 접근 요구사항을 가질 수 있다. 첫째, 사용자는 자신이 소유한 정보에 대해서 신뢰되는 사람만이 접근하기를 바란다. 둘째, 사용자의 리소스(resource)를 이용 시 자신과의 신뢰관계가 정립된 후 이용하기를 바란다. 셋째, 사용자는 자신이 정한 규칙에 의해 리소스를 이용하는 사용자의 행동을 제한하기를 바란다. 이러한 요구사항을 기초로 하여 OSN에서의 접근 제어는 정보 요청자의 활동 영역을 제한할 수 있는 유용한 도구로 활용되어 왔다. 하지만, Mandatory Access Control[1], Discretionary Access Control[2], Role Based Access Control[3] 등 전통적인 접근제어 방법을 OSN에 적용할 경우 제한사항이 있다. 전통적인 접근 제어 방법은 사용자간의 접근 허용의 범위가 미리 설정되어 있고, 인위적으로 수정을 하지 않으면 접근 제어의 범위가 변하지 않는다. 또한, 접근 제어의 범위가 사용자와의 관계에 따라서 고정이 되기 때문에, 관계를 맺을 당시 높은 허용범위를 부여받은 사용자가 후에 악의적인 행동을 한다고 해도 제약할 방법이 없다. 또한, OSN에서 사용자는 자신의 정보를 지속적으로 변경하고, 사용자간의 활동도 매번 다르게 하고 있다. 그러므로 본 논문에서는 기존의 OSN의 접근제어 방식의 문제점을 살펴보고, OSN의 특성에 맞추어 신뢰 중심의 접근제어를 제안토록 하겠다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 관련 연구와 기존 연구의 제한사항을 언급하고, 3장에서는 제안하는 동적 신뢰도 계산 알고리즘의 적용 방법을, 4장에서는 동적 신뢰도에 따른 접근 허용 범위의 할당 방법을 제안하겠다. 또한, 5장에서는 실험을 통해 동적 신뢰도 변경에 따른 변화하는 접근이 가능함을 평가 하고, 6장에서는 본 논문의 제안을 정리하고 향후 연구 과제를 기술하도록 하겠다.

II. 관련 연구

2.1 신뢰(trust)의 정의와 관련 연구

신뢰는 실제 사회에서나 가상세계에서 모두 중요한 사회적 관계의 일부이다. 우리는 누구와 의사소통을 할지, 자료를 공유할지 등 사회적 관계 속에서 행동의 결정을 내리게 되는데, 이때 신뢰를 이용하기도 한다. 신뢰 개념은 정성적이기 때문에 많은 연구에서는 정량적 개념인 신뢰도를 다음과 같이 정의하였다. L. Miu 등은 [4]에서 '신뢰도는 어떤 객체(entity)의 지난 행동으로 비추어 볼 때, 장차 예측될 행동에 대한 기대(expectation)' 라고 정의 하였으며, Gambetta 등은 [26]에서 "어떤 개인이 타인이 장차 그러한 행동을 할 것이라는 주관적인 확률적 기대" 라고 정의하였다. 신뢰는 하루아침에 결정이 되는 것은 아니므로, 다시 말하면 신뢰도는 위에서 언급한 바와 같이 지난 행동에 근거한 사용자가 가지고 있는 특정한 가치이며, 과거의 경험과 미래의 예측을 연결함으로써 관계 파트너간의 불확실성과 위험을 감소시키고, 높은 불확실성하에서도 위험을 공유할 수 있도록 하는 것을 의미한다.

신뢰의 가치 측정에 있어서 가장 중요한 주체는 신뢰를 평가받는 대상자와 그 인원의 신뢰를 평가하는 평가자로 나눌 수 있다. 각 인원과의 관계가 서로 직접적으로 알고 있는 사이라면, 평가자에 따라서 상대적인 가치를 부여할 수 있을 것이다. 하지만, OSN에서는 서로 알지 못했던 인원까지도 의사소통 및 자료

Table 1. Security threats related with trust in OSN

보안 위협	내 용
개별적인 악의적 사용자 (individual malicious peers)	정보 제공할 때, 항상 악의적으로 거짓된 정보를 제공하는 사용자
악의적 사용자 그룹 (malicious collectives)	같은 악의적인 사용자끼리 최고의 신뢰도 값을 부여하여 평판 시스템을 방해하는 그룹
위장된 악의적 사용자 그룹 (malicious collectives with camouflage)	악의적인 사용자 중 특정 부분만 악의적인 사용자 그룹을 조성하여 평판 시스템을 방해하는 그룹
시빌 공격 (Sybil Attack)	공격자가 다수의 신원 정보를 허위로 생성하고 이를 기반으로 시스템에 등록하는 악의적인 행동
먼저 신뢰된 악의적 사용자 (malicious pre-trusted peers)	예전에는 신뢰된 사용자였으나 후에 악의적인 사용자로 변하여 평판 시스템에 영향을 주는 사용자

공유를 해야 하기 때문에 상대방의 평가, 즉 추천이나 평판에 근거하여 신뢰도를 평가할 수 있다. 이러한 신뢰도를 평가하는 방법은 평가자가 평가하는 직접적이고 주관적인 평가와 다른 사람이 대상자를 평가하여 그 결과를 알려주는 간접적이고 객관적인 평가의 결합으로 생각할 수 있다.

특히, 여러 관계를 중요시 여기는 OSN에서 신뢰도는 의사소통을 결정하는 유용하고도 강력한 도구가 되어왔으며, 관련하여 신뢰도 계산을 위한 많은 연구가 진행되어 왔다. 예를 들어, Golbeck[6]은 Tidal-Trust 알고리즘을 제안하였다. 이 알고리즘은 신뢰자와 피신뢰자로부터 최단 사용자 관계 중 가장 높은 신뢰도를 보인 경로만을 판단하여 정보를 제공한다. 하지만, 해당 모델에서는 고정으로 할당된 정보만을 사용하므로, 동적인 현실세계의 적용은 어렵다. EigenTrust[7] 알고리즘에서는 사용자 경험을 통한 유일한 전역적 신뢰값(unique global trust)을 할당한다. 최고 높은 가치의 값을 가진 인원만 정보를 공유할 수 있도록 만들어 준다. 하지만, 때에 따라서는 각자 인원간의 거짓 정보를 만들어 줄 수 있으며, 전역적인 신뢰값을 사용하므로, 신뢰 측정에 대한 요소를 개인화하기 힘들다. PeerTrust[8]은 개인화된 유사도(similarity)와 피드백 정보에 대한 가중치를 부여하였다. 하지만, 계산 과정에서 전체 사용자 신뢰 정보에 의존을 하게 되어 계산상 많은 부하가 걸리며, 과거와 현재의 비중을 조절할 수 없다. Wen[9]은 직·간접적인 신뢰도의 비중을 선택하여 다루게 되었다. 이 모델의 단점은 시간이 경과함에 따라서 가중치가 변하지 않는다는 것에 있다. Y. Feng[10]은 진화하는 동적 신뢰도 모델을 제시하였다. 하지만, 진화의 방법이 모든 신뢰도에 대한 평균을 재계산함으로써 시스템 내 많은 부하를 가져 온다.

2.2 OSN의 신뢰도와 관련된 보안위협

소셜 네트워크의 이용자 수가 폭발적으로 증가하고, 각종 비즈니스에 활용되면서 소셜 네트워크의 보안에 대한 위협도 같이 증가하게 되었다. 악의적인 사용자는 OSN에서 떳떳 방법을 이용하여 신뢰와 평판을 조작하기도 한다. 평판을 올리기 위해서 거짓된 칭찬을 이용하기도 하도, 반대로 어떤 신뢰되는 사용자를 악의적으로 비난하기도 한다. 또한, 상황에 따라서 어떤 사용자는 자신에게 불리하면 거짓된 정보를 제공하기도 하고, 자신에게 유리하면 참된 정보를 제공하기도 한다. Table 1. 은 OSN에서 신뢰도와 관련된 보안 위협의 종류를 나타낸다[5].

2.3 기존 OSN 접근제어 연구 및 제한사항

현재 Facebook, Google+ 등 많은 OSN 에서는 사용자의 정보공유 통제를 위해서 접근 제어 방법을 사용하고 있다. 이러한 접근 제어는 public 또는 private 등의 강제적 접근제어 방법(Mandatory Access Control)[1]을 사용하기도 하고, 친구나 그룹 관계를 정의하여 역할 중심의 접근제어(Role Based Access Control)[3] 방식을 이용하기도 한다.

현실세계에 발맞추어 그동안 OSN의 접근 제어 방법에 관련하여 많은 연구가 진행되어 왔다. 규칙기반의 접근제어(Rule-based Access Control)[11,12]는 신뢰자가 규칙을 설정하여 피신뢰자에 대한 접근 통제를 한다. 규칙에 대한 기준은 관계 역할(relationship type), 사용자 관계의 떨어진 정도(relatinoship depth), 고정된 신뢰도(static trust

Table 2. Comparison the proposed dynamic trust access control model to previous access control models in OSN

구 분		신뢰측정 기준제공	다차원 관계	유사도 측정	제3자 의견 반영	가중치 변경	시스템 개인화	다단계 접근제어
기존 OSN 접근 제어	[11,12]	○	○	-	-	-	-	○
	[13]	-	○	-	○	-	○	○
	[14]	-	○	-	○	-	○	○
제안하는 모델		○	○	○	○	○	○	○

value)값을 사용한다. 하지만, 미리 설정된 신뢰도는 주관적 설정에 의한 고정 값이며 각 사용자들의 관계가 지속적으로 변화하는 OSN의 특성상 실시간 반영에는 무리가 따른다.

다자간 접근제어(Multiparty Access Control)[13], 관계 중심의 접근제어(URRAC)[14] 에서는 하나의 정보를 위해서 이를 보유하고 이용하는 사용자의 역할을 정보 소유자, 생산자, 사용자, 분배자 등 정보 이용자의 역할을 상대적인 의미로 분리하여 각각의 역할에서의 규칙을 절충하여 정보 공유하는 것에 중점을 둔다. 다자간 접근 제어나 관계중심의 접근제어에서 역할 중심의 규칙을 절충하여 각 역할에 대한 정보 유출을 방지할 수 있는 장점이 있지만, 반대로 역할 간 이해관계가 상충할 때에는 데이터 공유가 보류되는 단점이 존재하기도 한다.

위와 같은 방식의 OSN에서의 접근 제어 방법은 기본적으로 정적인 접근제어 방식으로 다음과 같은 단점을 지닌다. 첫째, 사용자간의 접근 허용의 범위가 미리 설정되어 있어 인위적으로 수정을 하지 않으면 접근 제어의 범위가 변하지 않는다. 둘째, 역할이나 관계 중심의 접근제어 방법은 개인 및 조직 간의 관계 조합이 복잡해지고, 다변화 되는 OSN의 특성을 제대로 반영할 수 없다. 셋째, 기존 접근제어 방법의 접근제어의 범위가 사용자와의 관계에 따라서 고정이 되기 때문에, 관계를 맺을 당시 높은 허용 범위를 부여받은 사용자가 후에 악의적인 행동을 한다고 해도 제약할 방법이 없다[23,24]. 그러므로 기존 OSN의 정적인 접근제어 방식에서 사용자의 동적 신뢰 변화를 이용하여 접근제어를 할 필요가 있다. Table 2. 는 제안하는 접근제어 모델에 대한 기존의 연구와 차이점을 나타내고 있다.

III. 동적 신뢰도 평가 방법

3.1 신뢰도(Trust) 산출을 위한 요인

OSN에서 구성원 간 소통은 대면 접촉과 같은 물리적 접촉이 없으며 느슨한 수준의 관계가 많기 때문에 서로에 대한 이해수준에 있어서 한계가 존재할 수밖에 없다. 하지만, 신뢰 구축은 관계발전의 한 형태로 OSN의 '사용자 쌍방의 반복된 상호작용 과정'을 통해서 상대방에 대해 예측 가능성이 높아지고, 상대방의 능력을 평가하면서 관계 의지를 형성하는 가운데 신뢰 형성이 가능하다.

신뢰 형성을 위한 주체는 기본적으로 신뢰자(trustor), 피신뢰자(trustee), 제 3자(third party)로 나눌 수 있다. 신뢰자는 피신뢰자와의 과거의 경험을 평가하여 자신의 정보에 접근 결정을 하는 주체이다. 피신뢰자는 자신이 신뢰자의 정보에 접근이 정당하고, 이를 인정하도록 자신을 표현하는 주체이다. 제 3자는 피신뢰자와의 과거의 경험에서 비롯된 신뢰도를 현재 신뢰자에게 제공하는 주체이다.

신뢰 평가를 위한 요인은 크게 내부적 요인과 외부적 요인으로 나눌 수 있다. 내부적 요인은 신뢰자와 피신뢰자 당사자 간의 관계에서 확인할 수 있는 요인이며, 외부적 요인으로는 당사자가 아니더라도 상대방의 추천이나 피신뢰자가 제 3자로부터 얻을 수 있는 명성같은 것이다. 기본적으로 아무런 연결이나 상대방을 알 수 없을 경우에는 신뢰도의 수준은 '영(0, Zero)' 에 가깝다. 하지만, 타인에게 들려오는 피신뢰자의 명성이나 추천으로 보았을 때 외부적인 요인을 통해 피신뢰자와의 신뢰관계가 성립된다. 이는 보통 미약한 상태로 신뢰자가 피신뢰자를 진정으로 신뢰를 하기 위해서는 내부적인 요인, 즉 피신뢰자 행동 평가를 통해 결정 가능하다.

그렇다면 신뢰를 쌓기 위한 선행 조건은 무엇인가? Mayer 등[25]은 신뢰의 선행요인을 종합한 대표적인 연구 결과에서 평가 요인으로 신뢰자의 성향과 능력, 피신뢰자의 성실성, 신뢰자와의 관계를 언급하고 있다. 물론 [4],[26] 등 신뢰 평가의 기준을 제시하는 많은 연구가 존재하지만, 본 연구에서는 OSN에서 사용자가 실제 서비스를 이용과 연계하여 판단하였을 때, Mayer가 제시한 대인 신뢰형성 요인은 접근 제

Table 3. Trust evaluation factors through OSN services

주체	평가 요인		정 의	가능한 소셜 네트워크의 서비스	
				긍정 측면	부정 측면
신뢰자 요인	내부적 요인	신뢰자의 성향 (ta, ts, tr)	타인에 대하여 믿을 만 하다고 생각하는 일반화된 기대로 이어지는 성격의 특성		
		능력(A)	특정 분야에 대한 경험과 능력, 지식 등 다른 사용자와 비교하여 해당분야의 경험과 능력이 뛰어난 정도	추천, 스크랩	비추천
피신뢰자 요인		성실성(S)	상대방의 행위에 있어서 오랜기간 동안 일관된 행동을 보이는 정도	방문 회수, 댓글, 메시지, 쪽지, 채팅	신고
		신뢰자와의 관계(R)	신뢰자와 상호작용 관계를 발전시켜 가면서 의사소통과 가치 공유 등 다양한 경험적 특성을 살릴 수 있는 가치	친구, 공통 친구, 공통 그룹	관계 차단
제 3자	외부적 요인	제 3자 추천 (*Indirect Trust*)	피신뢰자와의 상호작용 경험으로 비롯된 피신뢰자에 대한 신뢰에 대한 정도	제 3자의 신뢰도	

어를 위한 수치화 표현이 가능한 기준이 되므로 가장 타당하다고 판단된다. 그러므로 본 연구에서는 Mayer가 제시한 대인 신뢰형성 요인 연구를 바탕으로 Table 3.과 같이 신뢰 평가 기준을 제시하도록 하겠다.

신뢰 평가 요인의 특성은 다음과 같다. 먼저 신뢰자의 성향이다. 신뢰자 성향은 타인에 대해 믿을만하다고 생각하는 일반화된 기대로 이어지는 성격의 특성이다. OSN에서의 특정 서비스로 이어지지는 않지만, 피신뢰자의 행위를 판단하여 신뢰를 부여하는 가중치의 변수가 된다. 두 번째는 신뢰자의 능력이다. 이는 특정 분야에 대한 경험과 능력, 지식 등 다른 사용자와 비교하여 해당분야의 경험과 능력이 뛰어난 정도로 정의 되는데, 즉, 피신뢰자가 신뢰자를 믿고 의지하여 데이터에 대한 가치 공유를 할 수 있음을 의미한다. 세 번째는 피신뢰자의 성실성이다. 피신뢰자의 성실성은 오랜 기간 동안 피신뢰자가 신뢰자의 데이터에 일관된 피드백을 보이는 정도이다. 네 번째는 피신뢰자와 신뢰자와의 관계이다. 의사소통의 중심이 되는 관계는 서로 공통된 친구나 그룹을 통해 신뢰자와의 친밀감을 나타낼 수 있다. 마지막은 외부적 요인으로 제 3자의 추천을 들 수 있다. 제 3자가 과거 피신뢰자와의 신뢰형성을 현재 신뢰자에게 부여하여 신뢰자가 피신뢰자는 상대적으로 판단할 수 있는 기준을 마련해 준다.

3.2 동적 신뢰도 계산

3.2.1 신뢰 만족도(trust satisfaction)

신뢰 만족도는 신뢰자(P)가 피신뢰자(Q)가 사용하는 OSN의 서비스 기능에 대해서 신뢰평가를 하는 것이다. 이러한 신뢰 만족도는 다음과 같이 계산될 수 있다.

$$Sat_{current}(P,Q) = (ta\times A)+(ts\times S)+(tr\times R) \quad (1)$$
$$(\text{단}, 0<ta, ts, tr\le 1\text{이고}, ta+ts+tr=1\text{임})$$

ta, ts, tr은 해당 OSN의 서비스를 이용함에 있어서 신뢰자의 능력, 피신뢰자의 성실성, 신뢰자와의 관계에 대해 나타나는 신뢰자의 평가 성향이며, 이는 각 평가요소에 대한 가중치로 나타난다. 각 가중치의 합은 $ta+ts+tr=1$ 이 된다. A, R, S 는 2장에서 제시한 신뢰자의 능력, 피신뢰자의 성실성, 신뢰자와의 관계와 관련된 신뢰 평가 요소와 매칭이 되는 실제 OSN의 서비스를 나타내고 있다. 피신뢰자의 서비스 이용이 만족될 만한 수준이면 1이 되고, 안되면 0 이 된다. 부분적으로 신뢰 만족도에 대한 범위는 〔0, 1〕 이다. 각 신뢰 만족도는 시간에 따라 변화한다. 그러므로 시간(t) 에 따른 신뢰 만족도는 (2) 와 같이 나타낼 수 있다.

$$Sat_t(P,Q) = \alpha \times Sat_{current}(P,Q) + (1-\alpha) \times Sat_{t-1}(P,Q) \quad (2)$$

이때 α 는 현재 신뢰 만족도의 반영비율을 의미하고, 과거(t-1)의 만족도 비율 또한 피드백을 통해 반영을 한다.

3.2.2 유사도(similarity)

신뢰자와 피신뢰자의 속성 조건이 얼마나 만족되었는지 결정 되었다면, 신뢰자와 피신뢰자가 얼마나 비슷한지 알아볼 필요가 있다. 왜냐하면, 비슷한 특징을 가지고 있는 사람들끼리는 더욱 가까이 느끼고 신뢰가 가기 때문이다. 만약에 A와 B가 비슷한 속성을 가지고 있다고 가정하자. A가 C를 신뢰한다면, B도 C를 신뢰할 가능성이 높다[16]. 또한, 사회적으로 비슷한 무리끼리 친구가 되며, 서로의 공통된 친구가 많을수록 더 친밀하게 느끼게 때문에 A와 B 사이에의 공통된 친구를 찾아야 한다. 그러므로, 신뢰자와 피신뢰자 사이의 신뢰 만족도에 대한 평균 거리($Dist$)는 (3)과 같이 나타낼 수 있다.

$$Dist_t(P,Q) = \frac{1}{N} \sum_{x \in N} \frac{1}{Sat_t(P,x) \times Sat_t(x,Q)} \quad (3)$$

여기서 N은 신뢰자(P)와 피신뢰자(Q) 사이에 연결된 공통된 친구(x)의 수를 의미한다. 본 논문에서는 공통된 친구를 찾기 위한 방법으로 Breadth First Search[18]를 사용하여 최단 거리 내에 있는 신뢰 만족도 만을 계산한다. 이 결과를 근거로 유사도의 증감을 결정한다. 왜냐하면, 신뢰자(P)와 유사도가 비슷할수록 공통된 친구(x)가 피신뢰자(Q)를 평가한 신뢰 만족도 값이 더욱 신뢰를 할 수 있기 때문이다.

유사도(Sim)는 신뢰 만족도 거리 평균이 허용 임계치(γ) 와 비교하여 이보다 적어지면 시간이 지날수록 유사도는 올라가고, 이보다 높으면 유사도는 떨어진다. 또한, 유사도 업데이트 시 처벌과 보상을 위한 계수를 사용한다. Das 등은 [19]에서 신뢰도 측정을 위한 처벌과 보상의 개념을 유사도에 적용시켜 신뢰도 측정 방법을 개선하였다. 이 때, 처벌 계수(ρ)는 보상계수(τ) 보다는 많이 책정을 하는데, 이는 신뢰도가 천천히 올라가고, 빨리 떨어지는 특성을 반영하기 위함이다. 왜냐하면, 신뢰는 쌓기는 어려운 반면에 읽기는 쉽기 때문이다. 관련하여 [19]를 변형하여 유사도 측정을 위해 (4) 와 같은 공식을 이용한다.

$$Sim_t(P,Q) = \begin{cases} Sim_{t-1}(P,Q) + (\tau \times (1 - Sim_{t-1}(P,Q))) & \text{단, } Dist_t(P,Q) < \gamma \\ Sim_{t-1}(P,Q) - (\rho \times Sim_{t-1}(P,Q)) & \text{단, 이외의 경우} \end{cases} \quad (4)$$

(단, $0 < \gamma < \rho < 1$이며,
최대 $Sim_t(P,Q) = 1$이고,
최소 $Sim_t(P,Q) = 1$임)

만약 공통된 친구 $N=0$ 인 경우에는 $Dist_t(P,Q) = 0$ 으로 하며 최초 유사도(Sim) 의 값은 0.5로 한다.

3.2.3 직접 신뢰 평가(Direct Trust, DT)

직접 신뢰 평가는 신뢰자가 피신뢰자의 신뢰 만족도를 직접 평가함으로써 계산할 수 있다. 여기서는 신뢰자와 평가자가 동일하므로 유사도는 항상 1이 되어 반영할 필요가 없다.

$$DT_t(P,Q) = Sat_t(P,Q) \quad (5)$$

3.2.4 간접 신뢰 평가(Indirect Trust, IT)

간접 신뢰평가는 신뢰자(P)와 연결된 타 사용자가 피신뢰자(Q)와 과거 신뢰 만족도를 통해서 얻어진 평균 신뢰 만족도를 측정한 값으로 이는 간접적인 추천 시스템과 동일한 의미이다. 다시 말하면, 이는 신뢰자(P)가 정보제공을 위해 자신과 인접한 사용자에게 입소문을 물어보는 것과 같은 원리이다.

간접 신뢰도를 구하는 공식은 (6)과 같다. 이때에는 피신뢰자와 타 사용자의 신뢰 만족도와 유사도를 반영함으로써 신뢰자와의 상대적인 거리를 반영할 수 있다. $i \in adj(P)$ 의 의미는 P와 인접하고, Q와 트랜잭션이 있었던 모든 i를 의미한다.

$$IT_t(P,Q) = \frac{\sum_{i \in adj(P)} Sat_t(i,Q) \times Sim_t(i,Q)}{|i|} \quad (6)$$

3.2.5 최근 신뢰도(Recent Trust, RT)

최근 신뢰도는 피신뢰자가 정보 요청 시 행했던 신뢰도에 따른 계산 결과를 반영한다. 이때, 최근 신뢰

도를 구하기 위해서 직, 간접 신뢰도를 합성하여 반영한다. 최근 신뢰도를 구하기 위한 공식은 (7) 과 같다.

$$RT_t(P,Q) = \beta \times DT_t(P,Q) + (1-\beta) \times IT_t(P,Q) \quad (7)$$

β는 신뢰자(P)가 피신뢰자(Q)에게 했던 활동 횟수를 Q 와 관련된 모든 트렌젝션 횟수로 나눈 것으로, 신뢰자가 판단하기 위한 직접 신뢰도의 최소 반영 비율(v)을 포함한 것이다. 여기서 s는 B와 신뢰 만족도 계산을 위한 트렌젝션을 했던 모든 인원을 의미한다.

$$\beta = \begin{cases} v \ (\text{단}, \beta < v \text{인 경우}) \\ v + \dfrac{\sum \#of transaction(P,Q)}{\sum_{s \in S} \#of transaction(s,Q)} \\ (\text{단}, \beta \geq v \text{인 경우}) \end{cases} \quad (8)$$

3.2.6 동적 신뢰의 진화

OSN 환경에서 신뢰도는 지속적으로 변화한다. t 시간에 신뢰된 행동을 보였던 사용자가 $t+1$ 시간에 악의적인 사용자가 되기도 하고, t 시간에 악의적인 행동을 보였던 사용자가 $t+1$시간에 신뢰된 행동을 보이기도 한다. 그래서 신뢰도는 반드시 시간에 근거하여 진화하여야 한다. 사용자에 대한 신뢰는 어느 한 순간에 결정이 되는 것이 아닌 지속적으로 결과로 판단을 해야 한다. 좀 더 정확한 신뢰도 측정을 위해서 판단을 위해 동적 신뢰도(Dynamic Trust)는 과거의 신뢰도와 현재 신뢰도의 평균을 구해야 한다. 여기서 θ는 과거 신뢰도의 반영 비율을 의미한다.

$$Dynamic\ Trust_t = \frac{\theta \times RT_{t-1}(P,Q) + RT_t(P,Q)}{2} \quad (9)$$

IV. 제안하는 동적 신뢰 중심의 접근 제어 모델

4.1 신뢰도와 접근제어의 매핑

이번 장에서 우리는 세부적으로 구분된 동적 신뢰도 변화에 따른 접근 권한을 할당하는 방법을 기술하도록 하겠다. 먼저, 피신뢰자가 신뢰자 영역에서 활동할 수 있는 영역은 Table 4.와 같다고 가정을 하자.

Table 4. Classified user actions with trust level

접근 허용 ID	신뢰자 영역에서 가용한 활동	신뢰도 범위
0	∅	0
1	{read}	(0, 0. 4)
2	{like, dislike}	[0. 4, 0. 6)
3	{link, comment}	[0. 6, 0. 8)
4	{write contents, tag}	[0. 8, 0. 9)
5	{share}	[0. 9, 1)

접근 허용에 대한 ID는 Table 4.에서 분류된 신뢰자의 가능한 활동 영역에 따라 차등 분류 하였으며, 여기서 접근 허용 ID 가 높을수록 낮은 ID의 활동 영역을 포함한다. 또한, 이러한 접근 허용 ID는 동적으로 변화하는 신뢰도 범위에 따라서 할당이 되어 사용자의 영역에서 활동 범위를 제한하였다.

4.2 동적 신뢰 접근제어 모델의 적용 및 구조

동적 신뢰도 반영을 위한 접근제어 모델은 Fig.1. 이 접근 요청 관리 영역, 접근 제어 영역, 접근 피드백 영역의 세 가지 영역으로 나눌 수 있다. 접근 요청 영역은 주로 접근 피신뢰자의 접근을 위한 스케줄링을 담당한다. 신뢰도 계산중에 다른 접근 요청이 이루어지면, 잠시 제한하고, 해당시간에 정확한 신뢰도 계산이 됨을 보장한다. 접근 제어 영역은 3장에서 제시하였던 동적 신뢰도 계산이 되며, 이 신뢰도를 기반으로 4장에서 제시되는 접근 권한이 할당이 된다. 마지막으로 접근 피드백 영역에서는 접근이 할당 된 후 피신뢰자의 활동이 모니터링 되어 신뢰도 계산에 반영이 된다. 그 결과 최종적인 동적 신뢰 접근제어 모델의 구조는 Fig.2.와 같다.

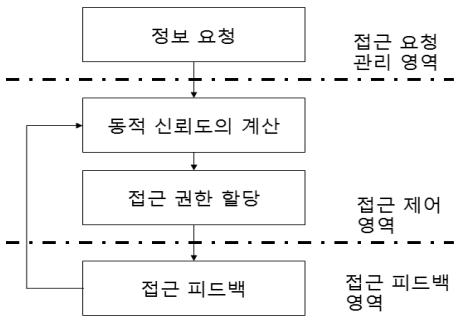

Fig.1. Proposed dynamic trust model

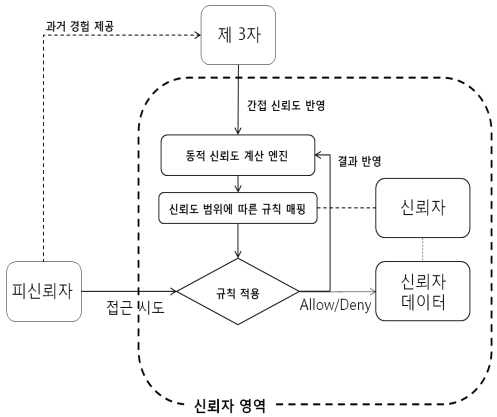

Fig.2. Proposed architecture for dynamic trust

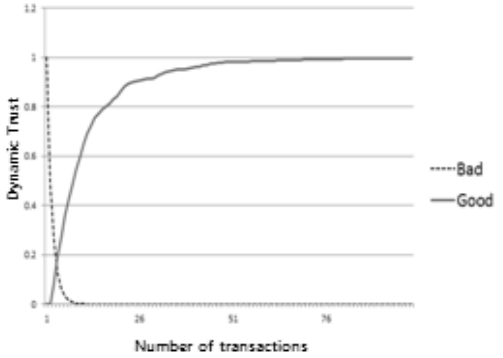

Fig.3. Dynamic trust by transactions

V. 실험 및 평가

5.1 실험 데이터 및 인자 설정

우리가 제안하는 접근 제어 방법을 평가하기 위해 Java 1.7 SDK[20] 과 Princeton 대학의 weighted digraph 및 Breadth First Search 패키지[21]를 이용하여 프로그램을 구성하였다. 또한, 실험을 위한 하드웨어 조건은 Intel Core i5 CPU 1.6Ghz의 CPU와 2.93GB의 주 기억장치를 활용하였다. 또한, 데이터는 무작위로 설정된 250명 사용자 규모의 작은 네트워크를 사용하였다[22]. 먼저 실험을 위한 인자 값의 셋팅은 Table 5.와 같다.

Table 5. Input variables for experiments

구 분	설 명	값
α	현재 신뢰 만족도 반영 비율	0.25
γ	신뢰 만족도 거리 평균 임계치	0.25
ρ	처벌 계수	0.06
τ	보상 계수	0.03
υ	최근 신뢰도 계산시 직접 신뢰도 반영 비율	0.25
θ	과거 신뢰도 반영 비율	1

5.2 실험 시나리오

5.2.1 시나리오 1 : 신뢰 만족도 변화에 따른 신뢰도 변화

우리는 실험 데이터에서 임의의 신뢰자와 피신뢰자를 설정하였다. 먼저, 긍정적인 신뢰 만족도를 지속적으로 제공하였을 경우와 부정적인 신뢰 만족도를 보였을 경우에 변화되는 신뢰도 추이를 확인 하였다. Fig.3.는 설정된 신뢰자와 피신뢰자의 신뢰도 결과를 얻기 위해 100번의 트렌젝션을 제공하였다. Fig.3.에서는 Bad는 부정적인 신뢰 만족도를 제공한 경우를 의미하며, Good은 긍정적인 신뢰 만족도를 제공한 경우를 의미한다.

긍정적인 신뢰 만족도와 신뢰도의 관계를 구하기 위해서, 초기 신뢰도 값을 0 으로 설정하였다. 왜냐하면, OSN에서 사용자 간에 한 번도 관계를 맺지 않았을 경우에는 서로 신뢰를 하지 못하기 때문이다. 하지만, 지속적으로 긍정적인 신뢰 만족도를 제공하면 신뢰도는 서서히 올라가게 된다. 반대인 경우에는 초기 신뢰도 값을 1로 설정하였다. 이는 부정적인 신뢰 만족도를 제공하면 반대로 급격히 내려가게 된다. 이러한 신뢰도에 대한 실험 결과는 사용자간의 신뢰 관계는 쌓기는 어려운 반면에, 잃기는 쉬운 사회적인 신뢰의 특성을 반영한 것이라 할 수 있다.

5.2.2 시나리오 2 : 전략적 속성 선택에 따른 신뢰도 변화

우리는 2장에서 언급되었던 보안 위협의 대표적인 경우를 볼 수 있다. 먼저 신뢰된 악의적인 사용자나, 위장된 악의적 사용자 그룹 등 자신의 이해 관계에 따라서 사용자가 전략적으로 속성 선택을 하는 경우를 들 수 있다. Fig.4.는 설정된 피신뢰자가 의도적으로 속성을 선택할 수 있다고 가정을 한 경우이다. 1000번의 트랜잭션 중에서 250번의 트렌젝션 마다 긍정적, 부정적인 신뢰 만족도의 변화를 설정 하였다.

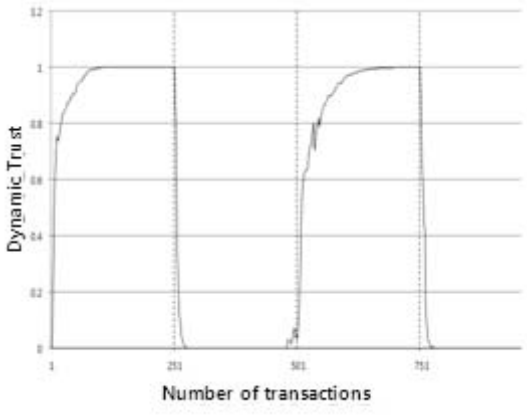

Fig.4. Trust changes by user's strategic actions

예를 들어, 트렌젝션 〔0, 250) 까지 긍정적인 신뢰 만족도를 선택한 경우이고, 〔250, 500) 까지 부정적인 신뢰 만족도를 제공하는 것이다. Fig.4.의 결과에서 최고 및 최저 점수의 신뢰 만족도를 선택적으로 제공하였다. 왜냐하면, 악의적인 사용자는 단시간에 신뢰도를 높이기 위해서 노력을 하기 때문이다. 하지만, 악의적인 사용자가 단 시간에 신뢰도를 높이기 위해서 시간적인 제약사항이 있다. 동적 신뢰도는 기존의 결과를 반영하여 현재까지의 신뢰도를 산출하기 때문이다.

5.2.3 시나리오 3 : 신뢰도 변화에 따른 접근 권한 할당

신뢰도에 따른 접근 제어 모델을 적용하기 위해서 시나리오 2에서 적용하였던 전략적인 속성 선택에 따른 만족도 변화를 선택하였다. 사용자의 악의적인 활동이 지속되면 신뢰도가 급격이 하락한다. 그러므로 할당되는 접근 권한의 범위도 급격히 축소가 된다. Fig.5. 는 전략적 선택에 따른 접근 권한의 변화를 나타내고 있다. 여기서 신뢰 만족도에 따라 신뢰도가 상승하면 사용자의 접근 권한의 영역이 넓어짐을 알 수 있다.

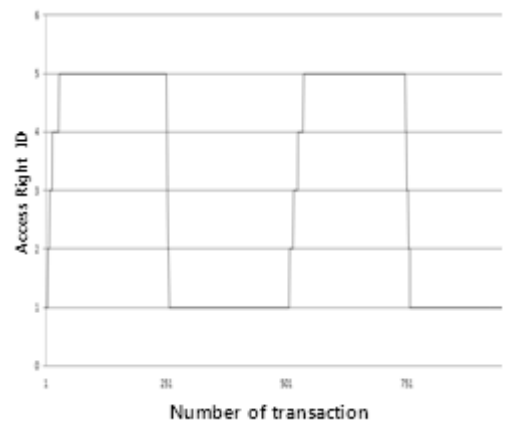

Fig.5. Conversion of user's trust level into access control level by the strategic selection

VI. 결론 및 향후 연구 과제

본 논문에서 우리는 속성 변화에 따른 신뢰도 변화와 신뢰도 변화에 따른 접근 권한이 변경됨을 살펴보았다. 이로써 동적 신뢰도는 접근 권한을 부여할 수 있는 판단 기준을 위한 중요한 도구임이 확인 되었다. OSN에서 사용자 간의 관계 및 활동은 지속적으로 변화하기 때문에, 전통적인 방법으로 접근 제어하는 것은 많은 제한사항이 존재 한다. 본 논문에서 접근 제어를 위한 동적 신뢰 기준을 적용함으로써 신뢰 만족도 변화에 따른 접근 제어가 가능함을 확인하였다. 또한, 현실 세계와 비슷한 신뢰 평가를 위해서 신뢰 만족도와 유사도를 적용함으로서, 사용자 사이에 판단하는 기준에 대한 상대적인 결과도 반영하였다. 하지만, 어떠한 속성이 중심이 되어 신뢰도에 영향을 미치는지 확언을 할 수 없다. 또한, 악의적인 사용자를 판단할 수 있는 기준도 명확하지 않다. 향후 이에 대한 추가적인 연구가 필요하다고 생각한다.

References

〔1〕 Qian, Xiaolei, and Teresa F. Lunt, "A MAC policy framework for multilevel relational database," IEEE Transactions on Knowledge and Data Engineering, Vol.8, No.1, pp. 1-14, 1996.

〔2〕 L.Snyder, "Formal models of capability-based protection systems," IEEE Trans. Computers, vol 30, pp. 172-181, 1981

〔3〕 R. S. Sandhu, E. J. Coyne, H. L . Feinstein, and C. E. Youman, "Role-based access control models," IEEE Trans. Computers, Vol. 29, pp. 38-47, 1996.

〔4〕 L. Miu, M. Mohtashemi, and A. Halbertstadt, "A computational model of trust

and reputation," 35th Annual Hawaii International Conference on System Sciences, IEEE, pp. 2431-2439, 2002.
〔5〕 Félix Gómez Mármol , Gregorio Martínez Pérez, "Security threats scenarios in trust and reputation models for distributed systems," Computers & Security, Vol. 28, Issue. 7, pp. 545 - 556, Elsevier, 2009.
〔6〕 J. Golbeck, "Computing and Applying Trust in Web-based Social Network," Ph.D Dissseration, Univ of Maryland, College Park, 2005
〔7〕 SS.D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P network," the 12th ACM international WWW conference, pp. 640-651, 2003.
〔8〕 L.Xiong and L.Li, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843-857, 2004.
〔9〕 L.Wen, P.Lingdi, L.Kuijin, and C. Xiaoping, "Trust model of users' behavior in trustworthy internet," in Proceedings of IEEE WASE International Conference on Information Engineering, pp. 403-406, 2009.
〔10〕 Y.Feng and W.Ying, "A reputation-based Dynamic trust Model for Large Scale Distributed Environment," Journal of Computational Information Systems, vol 9, no 3, pp. 1209-1215, 2013.
〔11〕 Barbara Carminati , Elena Ferrari and Andrea Perego, "Enforcing access control in Web-based social networks," ACM Transactions on Information and System Security (TISSEC), vol.13, no.1, pp.1-38, 2009.
〔12〕 B. Carminati, E. Ferrari, and A. Perego. "Rule-based access control for social networks," In On the Move to Meaningful Internet Systems 2006 Workshops, p 1734-1744. Springer, 2006.
〔13〕 H. Hu and G. Ahn. "Multiparty authorization framework for data sharing in online social networks," Data and Applications Security and Privacy XXV. Springer Berlin Heidelberg, pp. 29-43, 2011.
〔14〕 Cheng, Yuan, Jaehong Park, and Ravi Sandhu. "A user-to-user relationship-based access control model for online social networks," Data and Applications Security and Privacy XXVI, pp. 8-24, Springer Berlin Heidelberg, 2012.
〔15〕 Vincent C. Hu, David Ferraiolo and Rick Kuhn"Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)", NIST Special Publication 800-162, pp. 12-18, 2013.
〔16〕 Jøsang, Audun, Roslan Ismail, and Colin Boyd. "A survey of trust and reputation systems for online service provision," Decision support systems,Vol. 43,No. 2 pp. 618-644, 2007.
〔17〕 http://en.wikipedia.org/wiki/Euclidean_distance
〔18〕 http://en.wikipedia.org/wiki/Breadth-first_search
〔19〕 Das, Anupam, and Mohammad Mahfuzul Islam. "Securedtrust: A dynamic trust computation model for secured communication in multiagent systems." Dependable and Secure Computing, IEEE Transactions on, vol 9. no2, pp 261-274, 2012
〔20〕 http://www.oracle.com/technetwork/java/javase/downloads/index.html
〔21〕 http://algs4.cs.princeton.edu/home/
〔22〕 http://algs4.cs.princeton.edu/43mst/mediumEWG.txt
〔23〕 J. R. Douceur, "The Sybil Attack," Proc. Revised Papers from 1st International Workshop Peer-to-peer Systems(IPTPS 02), LNCS 2329, pp.215-260, Springer, 2002.

〔24〕 M. Castro, "Secure Routing for Structured Peer-to-Peer Overlay Networks," ACM SIGOPS Operating Systems Review, pp.299-314, Winter. 2002.
〔25〕 Mayer, R. C., Davis, J. H., and Shoorman, F. D., "An intergration model of organizational trust,"The Academy of Management Review, Vol. 20, No. 3, pp. 709-734, 1995.
〔26〕 Gambetta, "Conspiracy among the many: the mafia in legitimate industries," The economics of organized crime, Cambridge: Cambridge University Press, pp. 116 - 136, 1995.

〈저자소개〉

백 승 수 (Seungsoo Baek) 정회원
2002년 3월: 육군사관학교 전산학과 학사
2007년 9월: 미. 해군대학원(Naval Postgraduate School) 전산학과 석사
2009년~2012년: 제 3 야전군 사령부 참모
2012년~현재: 고려대학교 정보보호대학원 박사과정
2012년~현재: 육군사관학교 전자정보학과 정보과학 강사
〈관심분야〉 정보보증, 접근제어, 사이버전

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년: KISA(舊한국정보보호진흥원) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 정보보호대학원 정교수
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2004년~현재: 한국정보보호학회 이사
2010년~현재: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: SK커뮤니케이션즈 보안강화 특별자문위원
2012년: 중앙선거관리위원회와 서울시장후보 홈페이지 사이버테러 특별검사 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security