DOI: 10.3745/KIPSTC.2010.17C.1.015

신뢰도와 위험도로부터 합성된 지표에 기반을 둔 온라인 소셜 네트워크를 위한 접근 제어 방법

서 양 진† · 한 상 용††

요 약

'페이스북'이나 '마이스페이스'같은 소셜 네트워크는 사람들끼리 관심사를 공유하거나 인간관계를 유지·확장할 수 있는 유용한 도구로 인식되고 있다. 그러나 한편으로 소셜 네트워크를 통해 개인정보가 유출될 위험이 있으므로 이를 해결할 수 있는 방안이 필요하다. 기존 소셜 네트워크 사이트들이 접근 제어 방식을 통해 사용자 스스로 자신의 정보를 보호토록 하고 있으나 접근을 허용한 사람을 통해 제삼자로의 정보 유출이 가능하다는 점에서 효과적인 해결책이 되지 못한다. 온라인 소셜 네트워크의 특성 상 자신이 잘 알지 못하는 사람에게 정보 접근을 허용하는 경우가 자주 발생하는 데 여기에는 정보 유출의 가능성이 내포되어 있다. 이러한 문제에 대한 해결책으로 타인에 대한 신뢰도에 기반을 둔 접근제어 방법이 사용될 수 있으나 이러한 방식 또한 정보 유출의 객관적 위험성을 반영하지 못한다는 한계를 가진다. 이에 본 논문은 이러한 문제에 대한 해결책으로 신뢰도와 정보 유출 위험도를 합성한 지표를 기반으로 접근 제어를 수행하는 방법을 제안하였으며, 다양한 실험을 통해 정보 유출 위험도가 온라인 소셜 네트워크에서의 접근 제어에서 중요한 역할을 할 수 있음을 보였다.

키워드 : 접근 제어, 개인정보보호, 온라인 소셜 네트워크, 정량적 모델, 신뢰도, 위험도

An Access Control Method Based on a Synthesized Metric from Trust and Risk Factors for Online Social Networks

Yangjin Seo† · Sangyong Han††

ABSTRACT

Social Networks such as 'Facebook' and 'Myspace' are regarded as useful tools for people to share interests and maintain or expand relationships with other people. However, they pose the risk that personal information can be exposed to other people without explicit permission from the information owner. Therefore, we need a solution for this problem. Although existing social network sites allow users to specify the exposing range or users who can access their personal information, this cannot be a practical solution because the information can still be revealed to third parties through the permitted users albeit unintentionally. Usually, people allow the access of unknown person to personal data in online social networks and this implies the possibility of information leakage. We could use an access control method based on trust value, but this has the limitation that it cannot reflect the quantitative risk of information leakage. As a solution to this problem, this paper proposes an access control method based on a synthesized metric from trust and risk factors. Our various experiments show that the risk of information leakage can play an important role in the access control of online social networks.

Keywords : Access Control, Personal Information Protection, Online Social Networks, Quantitative Model, Trust, Risk

1. 서 론

1.1 온라인 소셜 네트워크의 개인정보보호 문제

관계를 지향하는 인간의 성향은 온라인 소셜 네트워크의 예상을 뛰어 넘는 성공으로 이어지고 있으며, 사람들은 자신의 관심사나 일상 등을 관리하거나 타인과 공유하기 위해 온라인 소셜 네트워크를 사용하고 있다. 그러한 결과로 온라인 소셜 네트워크에는 방대한 개인 정보가 존재하게 되었으며 이러한 데이터들은 향후 여러 분야에서 활용될 것으로

※ This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the HNRC (Home Network Research Center) - ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2009-C1090-0902-0035) and also partially supported by National Research Foundation of Korea Grant funded by the Korean Government (2009-0076290).
† 정 회 원 : 중앙대학교 컴퓨터공학부 박사수료
†† 종신회원 : 중앙대학교 컴퓨터공학과 교수
논문접수 : 2009년 9월 21일
수 정 일 : 1차 2009년 12월 24일
심사완료 : 2010년 1월 2일

예상되고 있다 [1, 2].

온라인 소셜 네트워크의 사용자 그 누구도 자신의 개인정보가 원치 않는 누군가에 의해 열람되거나 원치 않는 누군가에게 전달되는 것을 바라지 않을 것이다. 그럼에도 불구하고 온라인 소셜 네트워크의 각 사용자들이 온라인 공간에 존재하는 자신의 정보를 관리하는 일에 주의를 기울이지 못하는 경우가 많다. 페이스북에 있는 카네기 멜론 대학 소셜 네트워크에 대해 이루어진 조사[3]에 의하면 이용자들이 자신의 다양한 개인정보를 명시적으로 공개하고 있음을 알 수 있다. 또한 사용자가 명시적으로 자신의 정보를 공개하지 않았더라도 다른 정보를 통해 이를 추론할 수 있는 가능성도 존재한다 [4, 5]. 예를 들어 어떤 사람이 자신의 나이 정보에 대해 '공개하지 않음'으로 설정했다 하더라도 그 사람의 친구들이 대부분 20대라면 해당 사용자의 나이는 20대일 가능성이 높다. 결론적으로 온라인 소셜 네트워크는 자신의 공간이 안전할 것이라는 사용자들의 일반적인 기대와는 달리 현재 개인정보에 대한 적절한 보호를 제공하지 못하고 있다 [6].

1.2 온라인 소셜 네트워크의 접근제어 문제

온라인 소셜 네트워크에서는 개인정보 노출이 자연스럽게 발생하므로 이에 대한 보호 수단이 제공되어야 한다. 기존 온라인 소셜 네트워크 사이트들이 제공하는 개인정보보호 방식은 사이트마다 상이하나, 대부분 접근 제어를 이용하고 있다. 접근 제어는 정보보호 분야에서 기밀성 보호를 위해 일반적으로 사용하는 방식인데, 온라인 소셜 네트워크에 적용함에 있어 몇 가지 고려해야 할 사항이 있다 [7, 10-12].

첫째, 보호 대상의 범위이다. 각 사용자의 온라인 공간에 존재하는 개인정보에는 서비스 가입 시 입력하는 나이, 성별, 주소 등의 명시적인 개인 프로파일 데이터와 개인이 남기는 글이나 사진 등에서 얻어지는 데이터가 있다. 이러한 데이터 중 집 주소나 핸드폰 번호 같은 것은 민감도(sensitivity)가 높으며 선호하는 영화 장르 정보 같은 것은 민감도가 낮다. 사용자는 이처럼 상이한 민감도를 가지는 데이터들이 차등적으로 제어되기 원한다.

둘째, 온라인 소셜 네트워크의 접근 제어가 실세계를 반영한 것이 되기 위해서는 사용자간의 관계에 기반을 둔 접근 제어가 가능해야 한다. 정보의 소유자는 자신과 좋은 관계를 유지하는 사람에게는 넓은 범위의 데이터 접근을 허용하려 하지만 그렇지 않은 사람에게는 정보 접근을 제한적으로 허용하고 싶어 한다.

셋째, 온라인 소셜 네트워크상의 접근 제어에 있어 한 가지 더 고려해야 할 점은 사용자가 자신과 직접적인 관계가 없는 사람에게 데이터 접근을 허용하는 경우가 있다는 것이다. 사람에 따라서는 온라인 소셜 네트워크가 오프라인의 소셜 네트워크를 그대로 옮겨놓은 것일 수 있으나, 어떤 사람은 온라인을 통해 자신의 소셜 네트워크가 확장되는 것을 기대한다. 실제로 온라인 소셜 네트워크에서는 잘 알지 못하는 사람을 자신의 친구로 등록하는 경우가 존재한다. 또한 많은 온라인 소셜 네트워크에서는 '친구의 친구 (friend of friends)'라는 간접 관계에 대해서도 데이터 접근을 허용하도록 하는데, 이는 자신이 전혀 알지 못하는 사람에게 데이터 접근을 허용하는 결과로 이어질 수 있다. 한국의 대표적인 소셜 네트워크 사이트인 싸이월드의 경우에도 '친구'에 해당하는 '일촌' 관계가 존재하며 일촌 관계가 아니라 하더라도 방문자가 남긴 글이나 링크를 통해 다른 사람의 개인정보를 취득하는 것이 가능하다. 따라서 온라인 소셜 네트워크의 접근제어 방안은 간접 관계에 의한 개인정보 유출 가능성을 고려한 메커니즘이어야 한다.

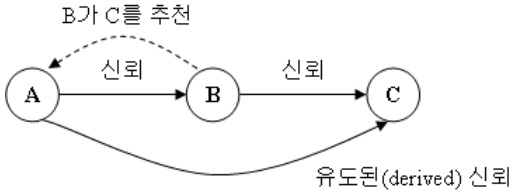
본 논문은 이러한 세 개의 요구사항 중 두 번째와 세 번째 항목에 관련된 문제를 다루고자 한다. 첫 번째 요구사항과 관련해서는 실제 공유의 대상이 되지 않는 정보는 배제된다고 가정하였다. 예를 들어 사용자의 주민등록번호와 같은 정보는 온라인 소셜 네트워크상에서 공유될 가능성이 희박하다.

본 논문은 접근제어의 문제를 다루고 있으므로 아이디 도용이나 해킹 등을 통한 개인정보 유출 문제는 본 논문이 다루고자 하는 영역이 아니다. 예를 들어 싸이월드를 통해 사생활이 원치 않는 누군가에게 알려지는 것은 아이디 도용이나 해킹 등에 의해 발생하기도 하지만, 자신이 명시적으로 공개 또는 공유한 글이나 사진 등을 통해서 발생하기도 한다. 본 논문은 후자의 문제를 다루고자 한다. 다시 말해 우리는 온라인 소셜 네트워크의 특성 상 자연스럽게 발생하는 정보 공유와 정보 접근 허용에 의해 발생하는 개인정보의 유출을 막는 방안을 제안하고자 한다.

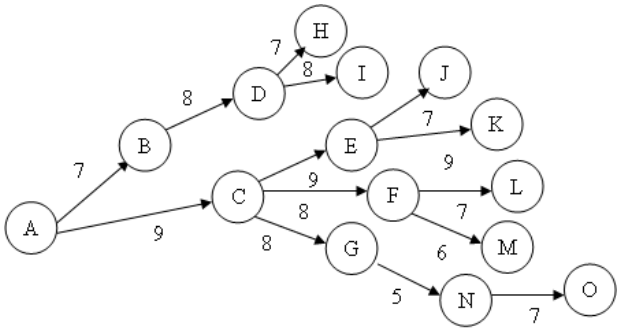
1.3 온라인 소셜 네트워크의 접근제어 문제에 대한 본 논문의 제안

사용자간의 관계 정도를 평가할 수 있는 요소에는 신뢰도, 친밀도, 관계의 종류, 관계 유지의 기간 등 여러 가지가 있겠으나, 접근 제어라는 관점에서 봤을 때 '신뢰도'가 유용한 항목으로 사용될 수 있다. 즉 자신이 타인에 대해 가지는 신뢰의 정도에 따라 접근 제어가 이루어진다면 이는 실세계에 근접한 방식이 될 것이다.

간접 관계를 가지는 사람에 대한 정보 접근 허용 문제에는 '신뢰 전이의 원리[13]'를 이용하고자 한다. (그림 1)은 신뢰 전이의 원리를 보여주고 있다. (그림 1)에서 원은 사람을 나타내고 화살표는 신뢰의 방향성을 나타내는 데, 사람 A는 사람 C와 간접 연결되어 있어 C의 신뢰도를 평가할 수 없으나 자신이 신뢰하는 직접 연결된 B의 추천에 의해 C를



(그림 1) 신뢰 전이의 원리



(그림 2) 신뢰도와 정보유출 위험도

신뢰하기로 결정할 수 있다. 이처럼 신뢰 전이의 원리를 적용하면 간접 연결된 사람의 신뢰도를 평가할 수 있고 이를 기반으로 접근 제어를 수행하는 것이 가능해진다.

그런데 이러한 신뢰도 기반의 접근 제어는 각 사람이 가지는 객관적인 정보 유출 위험도를 나타내지 못한다는 것에 그 한계가 있다. (그림 2)와 같이 사용자들이 자신의 이웃에 대해 가지는 신뢰도를 1에서 10까지의 숫자로 나타냈다고 가정해 보자 (큰 값일수록 신뢰도가 높은 것을 의미한다). 사람 A는 사람 B보다 C에게 높은 값을 부여함으로써 자신이 B보다 C를 더 신뢰함을 나타내고 있다. 그런데 만약 A, B, C 모두가 '친구의 친구'에게 데이터 접근을 허용했다면 C를 통해 A의 데이터에 접근할 수 있는 사람의 수가 B를 통해 A의 데이터의 접근할 수 있는 사람의 수의 3배가 된다. 이러한 상황에서 A가 자신의 이웃에 대해 주관적으로 부여한 신뢰도 값을 정보 접근을 허용하는 유일한 근거로 사용하는 것은 적합하지 않다. 온라인 소셜 네트워크에서의 접근 제어가 보다 효과적인 것이 되기 위해서는 각 사람이 가지는 정보 유출 위험도를 객관적으로 평가하고 이를 반영할 수 있는 방안이 필요하다. 이에 본 논문은 정보 검색 분야에서 각 웹 페이지가 가지는 중요도를 평가하는 페이지랭크가 고리즘[18]의 메커니즘을 채용하여터각 사용자가 가지는 정보 유출 위험도를 확률적으로 평가하고 이 값을 신뢰도 값구'합성한 지표를 정의한 후 이를 기반으로 접근 제어를 수행하는 방법을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 '신뢰'의 개념과 신뢰도 정량화 방식의 분류를 기술한 후 온라인 소셜 네트워크의 접근 제어에 적합한 신뢰도 정량화 방식을 정의한다. 이어지는 3장에서는 온라인 소셜 네트워크에서 각 사용자가 가지는 정보 유출 위험도를 산출하는 방법을 제시한다. 4장에서는 신뢰도와 정보 유출 위험도를 합성하는 방법과 합성된 지표를 기반으로 접근 제어를 수행하는 방법을 기술하며 5장에서는 실험을 통해 제시한 방법의 유용성을 평가한다. 6장에서는 온라인 소셜 네트워크의 접근 제어에 대한 기존 연구를 정리하고 마지막으로 7장에서는 본 논문의 제안을 정리하고 향후 연구 과제를 기술한다.

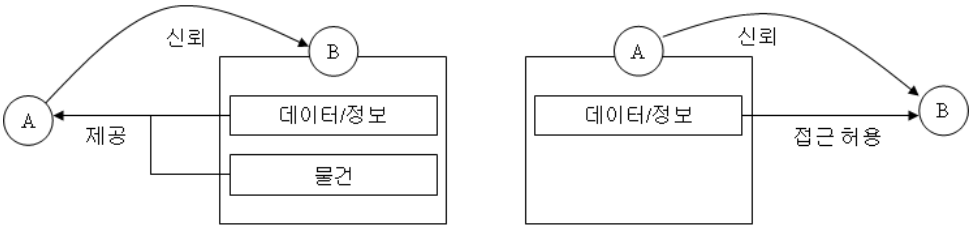
2. 온라인 소셜 네트워트의 접근제어에 적합한 신뢰도 모델

2.1 신뢰도의 정의

'신뢰도'는 사람이 어떤 선택을 내릴 때 이를 뒷받침하는 근거로 사용된다. 예를 들어 어떤 사람이 온라인 쇼핑몰에서 물건을 사고자 할 때 구매자가 판매자에 대해 가지는 신뢰도가 구매 결정에 있어 중요한 요소로 작용한다. P2P 파일 공유 시스템이나 추천 시스템에서도 데이터 소스를 선택하는 기준으로 신뢰도를 이용한다. 이처럼 신뢰도는 데이터나 물건의 제공자를 선택하는 기준으로 사용될 수 있는 데 본 논문에서는 이러한 상황에서 사용되는 '신뢰'의 개념을 '주제별 신뢰 (topical trust)'라고 정의한다. [7, 13, 14] 그런데 접근 제어에서 신뢰도를 사용할 경우 '주제별 신뢰'의 개념은 적합하지 않다. 왜냐하면 접근 제어에서는 신뢰도를 평가하는 사람과 데이터의 제공자가 동일하기 때문이다. 따라서 접근 제어에서의 신뢰도는 다른 사람이 나에게 해가 되는 행동을 하지 않을 것이라는 기대의 정도를 나타내는 것으로 생각할 수 있다. 본 논문에서는 이러한 상황에서 사용되는 '신뢰'의 개념을 '안전도 신뢰 (safety trust)'라고 정의한다. [7, 15]

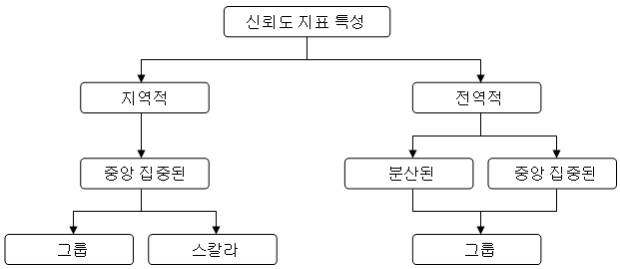
2.2 신뢰도의 정량화 모델

신뢰도가 여러 분야에서 유용한 도구로 주목받으면서 이를 정량화하는 다양한 방식이 제시되었다. 사람을 원으로 표시하고 사람 사이의 관계를 에지로 표시한다면 사람 사이의 신뢰도는 그래프를 구성하게 되고 신뢰도 계산 방식은 이러한 그래프에서 각 사람의 신뢰도를 정량적으로 계산해 낸다.



(a) 주제별 신뢰 (b) 안전도 신뢰

(그림 3) (a) '주제별 신뢰'와 (b) '안전도 신뢰'

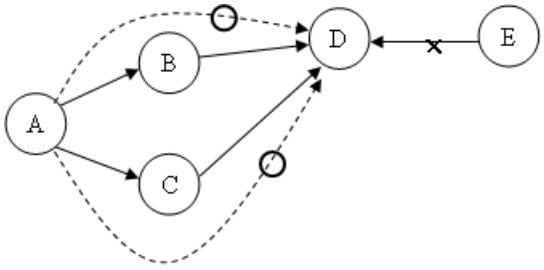


(그림 4) 신뢰도 지표 분류

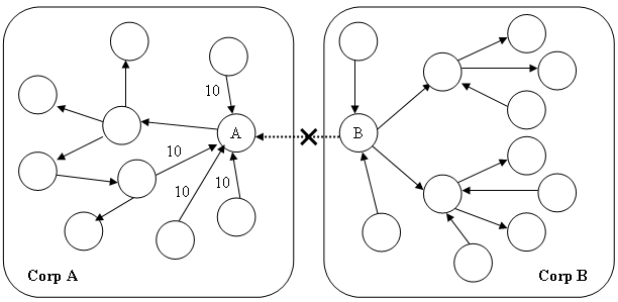
Ziegler는 [20]에서 여러 연구자들에 의해 제시된 신뢰도 계산 방법들을 체계적으로 분류하였는데, 이는 (그림 4)와 같은 특성 항목에 기반을 두고 있다. 여기서 '중앙 집중'과 '분산'은 신뢰도 계산이 이루어지는 위치에 관한 특성이다. 또한 '전역적(global)'은 신뢰도 지표가 그래프 전체 정보로부터 계산되는 것을 의미하고, '지역적(local)'은 신뢰도 지표가 그래프 정보 일부로부터 얻어짐을 의미한다. 연구자에 따라서는 지역적 신뢰도만이 개인화된 신뢰도 값으로서의 실제 의미를 가진다고 주장한다. [21] 이러한 주장은 (그림 5)에서 A가 D에 대한 신뢰도를 계산할 때 자신의 이웃인 B와 C의 의견은 참고하지만 자신과 관계없는 E의 의견을 반영할 필요가 없다는 생각에 기초를 두고 있다.

신뢰도의 계산이 전역적으로 이루어지는 것(또는 지역적으로 이루어지는 것)이 타당한지의 여부는 그것이 적용되는 상황에 종속적이다. 예를 들어 온라인 쇼핑몰의 경우 자신과 전혀 관계없는 사람들이 판매자나 제품에 대해 평가한 내용이 구매 결정에 중요한 근거로 사용된다. (이러한 경우에 사용되는 신뢰도를 '명성(reputation)'이라는 별도의 지표로 정의하기도 한다. [22]) 그러나 접근 제어에 있어서는 이러한 방식이 위험할 수 있다. 극단적인 예이기는 하나 (그림 6)에서 'Corp A' 회사의 직원들에 의해 높은 명성 값을 부여받은 'Corp A' 회사 직원 'A'를 'Corp B' 회사 직원 'B'가 자신의 회사 정보에 접근하도록 허용하는 것은 적합하지 않다.

마지막으로 '그룹'과 '스칼라'는 산출되는 신뢰도 값에 대한 특성이다. '스칼라'의 경우 소스로부터 목적지를 따라가며 단일 신뢰도 값이 산출되는 반면, '그룹'의 경우 신뢰도 값이 계산에 포함된 사람들 사이의 상대적인 순위(rank)로 산출된다. 웹 페이지의 중요도를 평가하는 페이지랭크 알고리즘



(그림 5) 지역적인 신뢰도 계산



(그림 6) 명성 지표에 기반을 둔 접근 제어의 위험성

[23]이나 Levien의 Appleseed[20]가 신뢰도를 그룹 지표로 산출하는 대표적인 알고리즘들이다.

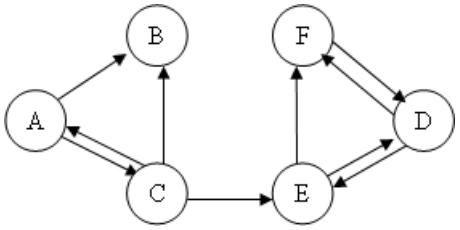
본 논문은 소셜 네트워크에서의 접근 제어 문제를 다루고 있으므로 '안전도 신뢰'에 해당하며, 신뢰도 계산이 지역적으로 이루어지는 것이 타당하다. 본 논문이 기여하고자 하는 바는 신뢰도와 정보 유출 위험도를 합성한 새로운 지표를 이용하여 소셜 네트워크에서의 접근제어를 수행하는 방법을 제시하는 것이므로 여러 신뢰도 지표를 적용하는 것보다는 단일의 신뢰도 지표와 정보 유출 위험도를 다양하게 조합하고 이에 따른 접근 제어 결과를 분석하는 방식이 적합할 것이다. 신뢰도 지표로는 지역적 스칼라 신뢰도 지표의 대표적인 알고리즘인 Golbeck의 TidalTrust[24]를 사용한다. TidalTrust의 정의는 다음과 같다.

$$t_{is} = \frac{\sum_{j \in adj(j) \mid t_{ij} \geq max} t_{ij} t_{js}}{\sum_{j \in adj(j) \mid t_{ij} \geq max} t_{ij}}$$

t_{is}는 사람 'i'가 사람 's'에 대해 가지는 신뢰도 값이며, *adj(j)*는 'i'의 이웃에 해당하는 사람을 말한다. 각 사람은 자신의 이웃에 대해 1부터 10까지의 자연수 값 중 하나를 신뢰도 값으로 부여한다. (값이 클수록 높은 신뢰도를 의미한다.) '$t_{ij} \geq$ max'는 'i'의 이웃들 중에서도 'i'가 가지는 신뢰도 값이 max 이상인 사람들의 의견만 반영하겠다는 것을 의미한다. TidalTrust는 원래 '주제별 신뢰'에 해당하는 신뢰도의 계산에 사용되나, '주제별 신뢰'와 '안전도 신뢰'의 신뢰도 계산에 있어 그래프 토폴로지는 동일하므로 TidalTrust를 이용하는 것이 가능하다.

3. 정보 유출 위험도 지표

(그림 7)은 작은 소셜 네트워크를 나타내는 그래프인데, 여기서 화살표의 방향은 한 사람이 다른 사람에게 자신의 정보 접근을 허용한 것을 나타낸다. 즉 사람 A와 사람 B의 경우 사람 A가 사람 B에게 정보 접근을 허용한 것이며 사람 A와 사람 C의 경우에는 상호간에 정보 접근을 허용한 것이다.



(그림 7) 작은 소셜 네트워크를 나타내는 그래프

(그림 7)의 그래프는 아래와 같은 특성을 가진다.

1) 방향성 있는 에지는 웹 페이지들 사이의 링크 연결을 나타내는 것과 동일하다.
2) 각 사람이 가지는 정보 유출의 가능성은 자신이 정보 접근을 허가해 준 직접 연결된 이웃 노드들의 정보 유출 가능성을 다 더한 값으로 정의할 수 있다. 예를 들어 사람 A의 정보 유출 가능성은 A가 정보 접근을 허용해준 사람 B와 사람 C의 정보 유출 가능성을 더한 값으로 정의할 수 있다.

1)과 2)에 의해 각 사람이 가지는 정보 유출의 가능성은 페이지랭크 알고리즘을 응용하여 모델링 할 수 있다. 우선 각 사람이 가지는 정보 유출 가능성을 구하는 기본 식은 아래와 같이 정의된다. [18]

$$r(P_i) = \sum_{P_j \in B_{P_i}} \frac{r(P_j)}{|P_j|} \quad (1)$$

사람 P_i의 정보 유출 위험도 $r(P_i)$는 P_i가 자신의 정보에 접근을 허용해 준 각 이웃 P_j의 정보 유출 위험도를 P_j에게 정보 접근을 허용해 준 이웃의 수로 나누어 얻은 결과 모두를 더한 값으로 정의된다. 각 사람의 정보 유출 위험도 값이 주어지는 것이 아니므로 소셜 네트워크에 존재하는 사람의 수가 n이라면 모든 사람의 정보 유출 확률은 1/n로 동일하게 정의된다. 이를 초기 값으로 하여 식 (2)와 같이 반복을 수행하면 각 사람의 정보 유출 위험도는 단일 값으로 수렴하게 된다.

$$r_{k+1}(P_i) = \sum_{P_j \in B_{P_i}} \frac{r_k(P_j)}{|P_j|} \quad (2)$$

사람들 사이의 정보 접근 허용에 따른 정보 유출 위험도 전파 관계를 행렬 H로, 각 사람의 정보 유출 위험도를 행벡터 R로 표시하면 식 (2)는 식 (3)과 같이 나타낼 수 있다.

$$R_{k+1} = R_k \times H \quad (3)$$

(그림 7)의 그래프에 대해 행렬 H는 다음과 같이 정의된다.

$$H = \begin{array}{c} \\ A \\ B \\ C \\ D \\ E \\ F \end{array} \begin{array}{c} \begin{array}{cccccc} A & B & C & D & E & F \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1/2 & 0 & 1/2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & 1/2 & 0 \end{pmatrix} \end{array}$$

이 행렬이 의미하는 바는 어떤 사람이 다른 사람에게 자신의 개인 정보에 접근할 수 있도록 허용하면 그 사람의 정보 유출 가능성의 일정 부분을 자신의 정보 유출 가능성에 추가하게 된다는 것이다. 3행 1열의 경우 사람 A만이 사람 C에게 정보 접근을 허용해 줬기 때문에 사람 C의 정보 유출 가능성의 전부를 사람 A의 정보 유출 가능성에 추가하게 된다. 사람 D의 경우 사람 E와 사람 F로부터 정보 접근 허가를 받았으므로 사람 E와 사람 F에게 자신의 정보 유출 가능성을 절반씩 나눠준다.

(그림 7)에서 각 사람의 정보 유출 가능성 초기 값은 1/6로 정의되고, 감쇠 인자(damping factor) 0.9를 적용하면 아래와 같은 행벡터로 수렴하게 된다.

(0.390686 0.016700 0.407190 0.069684 0.069684 0.048058)

결과적으로 (그림 7)의 소셜 네트워크에서 사람 C가 접근을 허용해 줬을 때 정보를 유출할 가능성이 가장 높으며, 사람 B가 가장 낮은 가능성을 가진다.

4. 신뢰도와 정보 유출 위험도의 합성 지표를 기반으로 한 접근 제어 방법

본 논문에서는 온라인 소셜 네트워크에서의 접근 제어를 위해 앞에서 제시한 신뢰도 값과 정보 유출 위험도 값을 합성한 지표를 이용하고자 한다. 그런데 신뢰도 값은 스칼라 값으로 정의되는 반면 정보 유출 위험도는 사람들 사이의 상대적인 순위로 정의되므로 둘의 합성을 위해서는 정보 유출 위험도를 스칼라 값으로 변환하는 과정이 필요하다.

정보 유출 위험도를 스칼라 값으로 변환하는 방식은 다음과 같다.

1) 1에서 10까지의 총 10단계의 안전도 레벨을 정의 (안전도 레벨 1이 가장 안전한 사용자 그룹임)
2) 각 사용자가 가지는 정보 유출 위험도 순위를 기준으로 사용자가 속하는 안전도 레벨을 결정
3) 안전도 레벨 1에 안전도 점수 (Risk-Free Score, 이하 RFS) 10을 부여 (안전도 레벨이 하나씩 증가할 때마다 RFS 1씩 감소, 안전도 레벨 10은 RFS가 1임)

안전도 레벨과 안전도 점수의 관계가 반드시 위의 정의와

같을 필요는 없다. 예를 들어 안전도 레벨과 안전도 점수를 동일시하는 것도 가능하다. 단 여기에서는 안전도 레벨 값이 작을수록 안전도가 높은 것으로 정의하였고 우리가 식 (4)에서 정의한 합성지표 HTRS는 값이 클수록 좋은 것으로 정의하였기에 안전도 레벨 1이 안전도 점수 10을 가지도록 정의하였다. 또한 안전도 점수는 계산 모델에 따라 다르게 정의될 수 있는 값으로 만약 HTRS의 최댓값을 1로 정의하였다면 안전도 레벨 1의 안전도 점수는 1이 되어야 한다.

정보 유출 위험도를 스칼라 값으로 변환하는 방식에서의 문제는 2)의 과정 즉 사용자가 가지는 정보 유출 위험도 순위에서 어떻게 안전도 레벨을 결정하는가이다. 이러한 문제에서 일반적으로 많이 쓰이는 방법은 대수 스케일(logarithmic scale)을 이용하는 것인데, 이를 적용할 경우 대다수의 사용자가 안전도 레벨 9와 10에 속하게 된다. 예를 들어 밑수(base) 7을 사용할 경우 약 3억 명의 사용자 중 98%가 안전도 레벨 9와 10에 속하게 되는 데, 이는 대다수의 사용자에 대한 간접 연결이 거부되는 결과로 이어질 수 있으므로 적합하지 않다. 본 논문에서는 이와 관련하여 전체 사용자 수를 10등분 하여 안전도 레벨을 부여하는 단순한 방식을 사용하였다. 정보 유출 위험도를 안전도 레벨로 변환하는 보다 정밀한 방식은 후속 연구를 통해 찾아내고자 한다.

사람 A가 B에 대해 가지는 직접 또는 간접 신뢰도 값을 TRS (TRust Score)라고 정의하면 합성된 지표 HTRS (Hybrid TRS)는 다음과 같이 정의된다.

$$HTRS(A, B) = \alpha \times TRS(A, B) + (1- \alpha) \times RFS(B), \quad 0 \leq \alpha \leq 1 \quad (4)$$

HTRS(A, B) 값은 상수 α에 의해 조절된다. α가 1인 경우 RFS는 HTRS 계산에 반영되지 않으므로 접근제어가 신뢰도 값에 의해서만 이루어지는 것이며, α가 0인 경우 접근제어는 안전도 점수에 의해서만 이루어지는 것이다.

마지막 단계로 우리는 HTRS 값에 기반을 둔 접근 제어 조건을 다음과 같이 정의하였다.

[정의] (접근 조건) 온라인 소셜 네트워크 OSN이 주어졌을 때, 접근 조건은 튜플 (v, α, HTRSth)로 정의된다. v는 정보 소유자가 직간접으로 연결되는 사용자이며, α는 TRS와 RFS의 볼록 결합(convex combination)에 사용되는 상수로 [0, 1]의 범위를 가진다. HTRSth는 접근이 허가되는 최소 HTRS 값으로 1에서 10 사이의 자연수 중 정보 소유자에 의해 결정된다.

일반적으로 접근 제어는 개별 파일이나 폴더 같은 단위(granularity)에서 이루어지나 본 논문에서는 특정 사람이 소유하는 데이터 전체에 대해 접근을 허용하거나 차단하는 것으로 가정하였다. 위에서 정의한 '접근 조건'을 소단위(fine-grained) 수준으로 확장하는 것은 어렵지 않다고 생각한다.

〈표 1〉 결과의 분류

정답 \ 판단	차단	허용
차단	True Positive (TP)	False Negative (FN)
허용	False Positive(FP)	True Negative(TN)

5. 실험 및 평가

5.1 실험 데이터 및 인자 설정

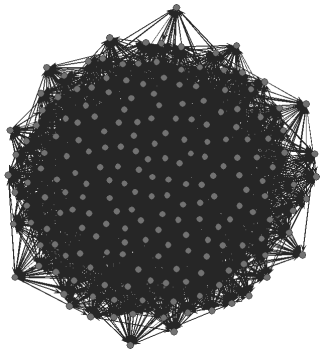
우리가 제안한 접근 제어 방법을 평가하기 위한 실험에 (그림 8)과 같은 소셜 네트워크를 사용하였다. 해당 소셜 네트워크는 총 200명의 사용자로 구성되며 밀도는 약 0.15이다. 어떤 사용자가 다른 사람에게 자신의 정보 접근을 허용한 경우 신뢰도는 1에서 10 사이의 무작위 값을 부여하였으며, 각 사용자의 정보 유출 위험도 계산에 감쇠 인자는 0.85를 적용하였다. 또한 간접 연결 신뢰도 계산에는 앞서 정의한 대로 TidalTrust 알고리즘을 이용하였다.

5.2 평가 방법

접근 제어에는 불확실성(uncertainty)의 문제가 수반되므로 [19] 성능 평가가 쉽지 않다. 여기서 불확실성이란 누군가에게 정보 접근을 허용했을 때 이것이 타당한 결정인지의 여부를 객관적으로 증명하는 것이 어렵다는 것을 말한다. 이에 본 논문에서는 다음과 같은 시뮬레이션을 통해 우리가 제안한 접근 제어 방법의 성능을 평가하였다.

1) 단계 1: 각 사용자가 다른 사용자에 대해 가지는 신뢰도 값을 생성함
2) 단계 2: 전체 사용자 중 일정 비율이 악의적인 사용자인 것으로 가정
3) 단계 3: 1)의 값을 입력으로 하여 간접 연결된 사용자에 대한 신뢰도 값 계산
4) 단계 4: 상수 α와 임계값 선택
5) 단계 5: 접근 조건에 따라 차단/허용 여부 결정

5)에서 나온 결과에 대한 성능 측정은 다음과 같이 수행



(그림 8) 실험에 사용된 작은 소셜 네트워크

하였다. 먼저 정보 소유자가 다른 사용자의 정보 접근을 차단하거나 허용하기로 결정한 결과를 <표 1>과 같이 네 가지로 분류하였다. 악의적인 사용자가 자신의 정보에 접근하려고 한다면 이를 차단하는 것이 옳다. 즉 어떤 사용자의 정보 접근을 차단하였는데 차단된 사용자가 악의적인 사용자였다면 이는 'True Positive'에 해당한다. 이에 반해 악의적인 사용자에게 정보 접근을 허용했다면 이는 'False Negative'에 해당한다. 또한 선의의 사용자를 차단했다면 'False Positive', 허용했다면 'True Negative'이다.

<표 1>의 분류를 바탕으로 '차단'과 '허용'에 대한 '정확도(Precision)'와 '재현율(Recall)'을 식 (5)에서 (8)과 같이 정의하였다. 여기서 N_v는 전체 꼭짓점의 수를 P_{bad}는 악의적인 사용자 비율을 나타낸다. 식 (5)에서 (8)은 모든 꼭짓점이 하나 이상의 들어오는 에지와 나가는 에지를 가지는 경우에 적용될 수 있다. (TP#, FN#, FP#, TN#은 순서대로 True Postive, False Negative, False Positive, True Negative에 해당하는 결과의 수를 말한다.)

- 차단의 정확도: $DP = TP\# / (TP\# + FP\#)$ (5)
- 차단의 재현율: DR = TP# / 차단되어야 하는 접근의 개수 (6)
  차단되어야 하는 접근의 개수 = $(N_v - 1) \times (N_v \times P_{bad})$
- 허용의 정확도: $AP = TN\# / (FN\# + TN\#)$ (7)
- 허용의 재현율: AR = TN# / 허용되어야 하는 접근의 개수 (8)
  허용되어야 하는 접근의 개수 = $N_v \times (N_v - 1) - (N_v \times P_{bad})$

5.3 실험 시나리오 및 결과

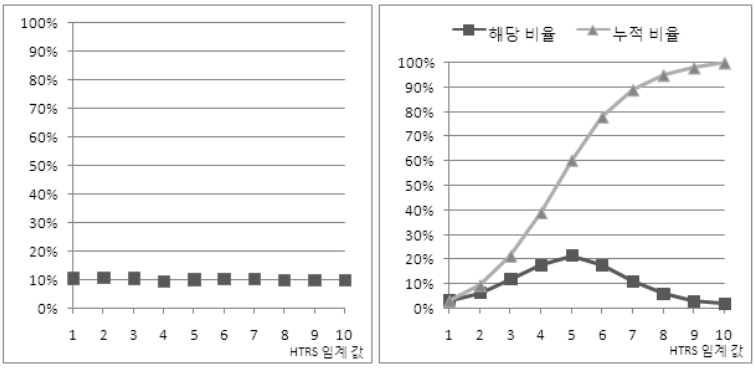
HTRS의 계산과 접근 조건에 있어 입력 변수는 '각 사용자들이 자신의 이웃(직접 연결된 사람)에게 부여한 신뢰도 값', α 값, 임계값(HTRSth), '안전도 점수' 총 4가지이다. 그런데 각 사용자의 안전도 점수는 네트워크 토폴로지에 의해 결정되고 본 실험에 사용된 소셜 네트워크는 하나(그림 8)이므로 각 사용자의 안전도 점수는 일정한 값을 가진다. 따라서 실험에서는 '각 사용자들이 자신의 이웃에게 부여한 신뢰도 값', α 값, 임계값(HTRSth) 3가지를 변화시키면서 결과를 구하였다.

실험은 총 3개의 시나리오로 구성되는데, <표 2>는 각 시나리오의 입력 변수 설정에 대한 설명이다. 각 사용자가 이웃에게 부여한 신뢰도는 무작위로 선택되었지만 <표 2>에 설명된 바와 신뢰도 값이 1부터 10까지 균등하게 분포하는 경우와 7이상의 값만이 사용된 경우 2가지를 실험하였다. 이는 신뢰도 값의 분포가 간접 연결 신뢰도 값에 영향을 주기 때문인 데, (그림 9)와 (그림 10)은 이러한 영향을 보여준다. 신뢰도의 분포가 편중된 경우를 실험에 포함시킨 것은 사람들이 다른 사람을 평가하는 것에 부담감을 가진다는 사실에 근거한 것이다. 예를 들어 eBay의 판매자와 구매자 간에 부여한 평점을 분석해 보면 좋은 평점을 주는 경우가 압도적으로 많다 [16, 17]. 따라서 시나리오 2와 3에 사용한 신뢰도 값의 분포는 실세계의 신뢰도 값 분포에 보다 근접한 것이라 할 수 있다.

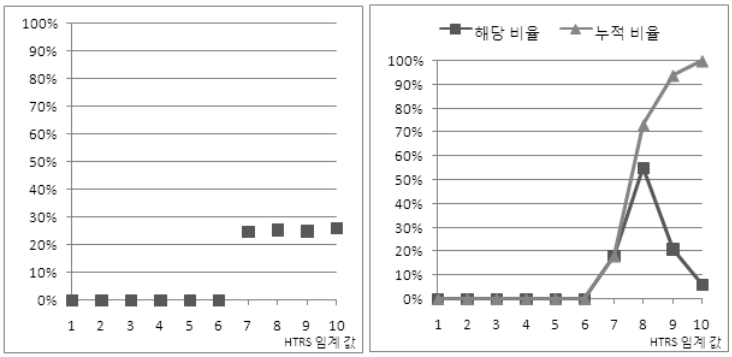
α 값은 시나리오 1과 2에서는 동일하게 1, 0.5, 0인 세 가지 경우를 실험하였으며, 시나리오 3은 α 값이 1, 0.2, 0인 세 가지 경우에 대해 실험을 수행하였다. 시나리오 2와 시나리오 3은 α 값을 제외하면 실험의 입력 변수가 동일하므로 α값이 결과에 미치는 영향을 분석하는 데에 사용될 수 있다. 각 시나리오의 성능 측정은 실험을 100회 이상 실행한 후 평균으로 제시하였다. 1회 실험마다 사용자 상호간의 신뢰도 값이 새롭게 생성되었고 악의적인 사용자는 5%만큼 무작위로 선택하였다. (그림 11)에서 (그림 16)은 3개의 시나리오에 대한 실험 결과를 보여주고 있다.

〈표 2〉 실험 시나리오별 입력 변수 구성 및 설정

입력 변수 / 구분	이웃에게 부여한 신뢰도 값	α	임계값
시나리오 1	1부터 10까지 균등한 비율로 생성	1, 0.5, 0	1부터 10까지 사용
시나리오 2	모든 신뢰도 값을 7 이상으로 생성 (7, 8, 9, 10의 분포가 균등함)	시나리오 1과 동일	시나리오 1과 동일
시나리오 3	시나리오 2와 동일	1, 0.2, 0	시나리오 1과 동일



(그림 9) 시나리오 1에 사용된 신뢰도 값의 분포와 TidalTrust에 의해 계산된 간접 신뢰도의 분포



(그림 10) 시나리오 2와 3에 사용된 신뢰도 값의 분포와 TidalTrust에 의해 계산된 간접 신뢰도의 분포

5.4 실험 결과 분석

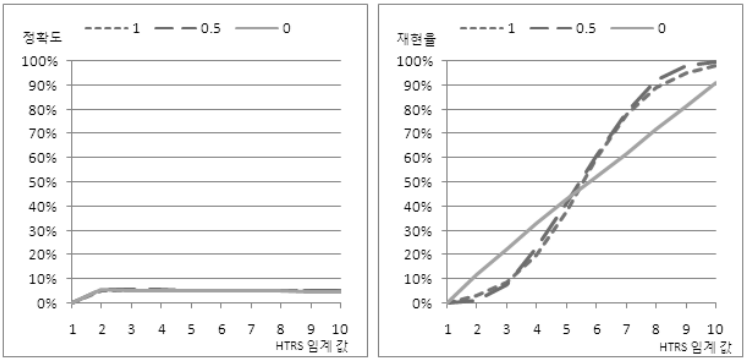
5.4.1 신뢰도 값이 균등한 분포를 가지는 경우 (시나리오 1)의 결과 분석

1) '거부'의 정확도와 재현율

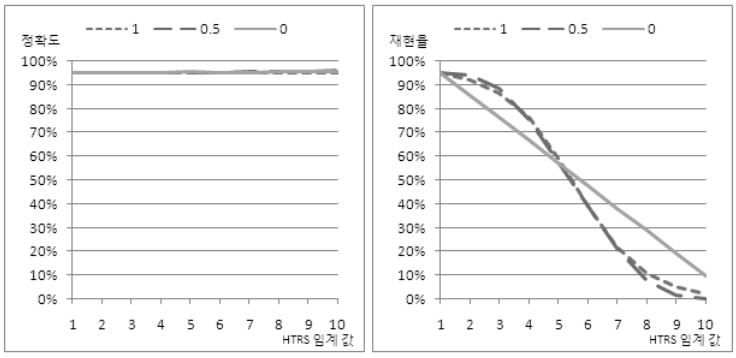
- '거부'의 정확도: (그림 11)의 2개의 그래프에서 알 수 있는 바와 같이 사용자가 선택하는 임계값과 상수 α에 상관없이 접근을 거부한 경우의 정확도는 약 5%이다. 임계값이 높아질수록 악의적인 사용자의 정보 접근을 거절하는 숫자(TP#)가 증가하나 허용해 주어야하는 사용자를 거절하는 경우(FN#)도 증가하므로 DP 값은 동일하게 나타난다. 이를 통해 알 수 있는 것은 접근제어에서 접근이 거부되는 사용자의 대다수가 선의의 피해자(접근이 허용되어야 하나 거부된 사용자)일 수 있다는 것이다.
- '거부'의 재현율: 접근 거부의 재현율은 임계값이 커질수록 증가하는 것을 (그림 11)의 오른쪽 그래프에서 볼 수 있다. 임계값이 커질수록 거부되는 사용자의 절대적인 숫자는 증가하게 되고 결과적으로 악의적인 사용자들의 정보 접근이 거부될 가능성이 증가하므로 이러한 결과는 당연한 것이다.

2) '허용'의 정확도와 재현율

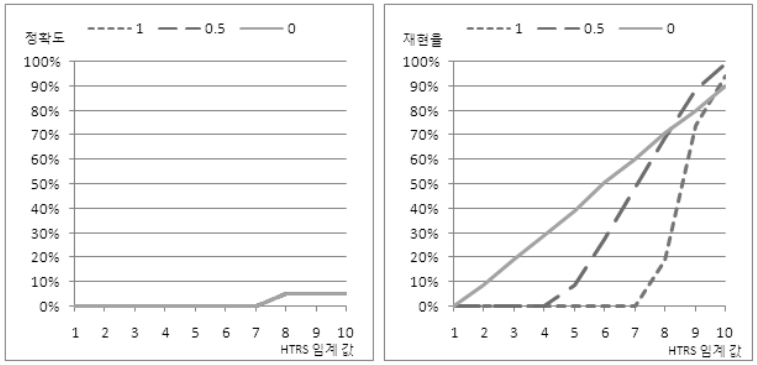
(그림 12)는 시나리오 1에서 접근을 허용했을 때의 정확



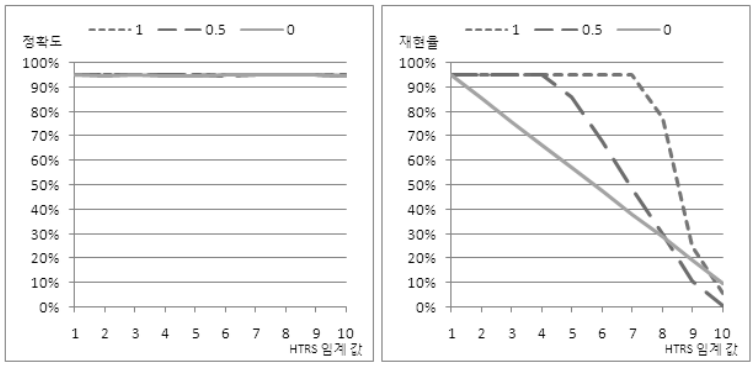
(그림 11) 시나리오 1에서 접근이 거절된 경우의 정확도와 재현율



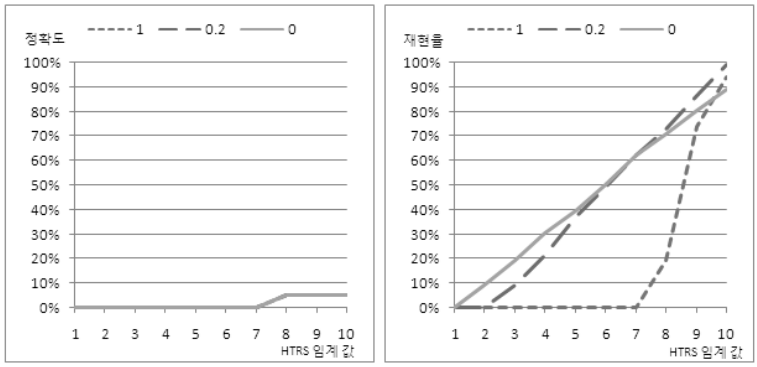
(그림 12) 시나리오 1에서 접근이 허용된 경우의 정확도와 재현율



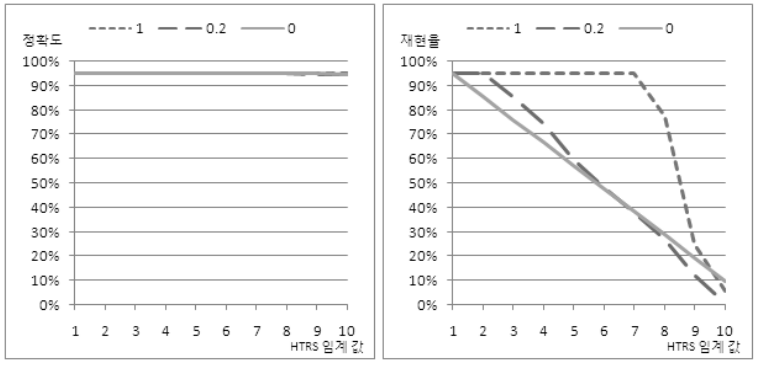
(그림 13) 시나리오 2에서 접근이 거절된 경우의 정확도와 재현율



(그림 14) 시나리오 2에서 접근이 허용된 경우의 정확도와 재현율



(그림 15) 시나리오 3에서 접근이 거절된 경우의 정확도와 재현율



(그림 16) 시나리오 3에서 접근이 허용된 경우의 정확도와 재현율

도와 재현율을 보여주는 데, (그림 11)과 비교했을 때 정반대의 패턴을 보임을 알 수 있다. 즉 정확도의 경우 사용자가 선택하는 임계값과 상수 α에 상관없이 95%로 일정한 값을 가지며 재현율은 임계값이 높아질수록 감소한다.

3) 결과에 대한 분석

- (그림 11)과 (그림 12)에 제시된 4개의 그래프는 접근제어 방식이 가지는 한계를 그대로 보여주고 있다. 즉 접근 제어 조건을 엄하게 가져갈수록 악의적인 정보 접근을 차단할 가능성은 높아지나 선의의 피해자가 발생할 가능성 또한 높아져서 정보의 원활한 유통과 공유가 어려워지는 문제점을 가진다. 물론 본 실험은 모든 사용자간에 직간접 연결이 존재하여 모든 사용자간 상호 정보 접근이 일어나는 경우에 대해 평가를 수행한 것이므로 이들의 부분집합에 대해 성능 측정을 하면 결과가 달라질 것이라 생각한다. 이처럼 모든 사용자 사이에 직간접 연결이 존재하는 것은 간접 연결의 거리에 제약을 두지 않았기 때문이므로 후속 연구에서는 HTRS의 계산 인자에 거리를 포함시킬 예정이다.
- 시나리오 1에 대한 실험 결과를 통해 직접 신뢰도 값이 균등한 분포를 가질 때 간접 신뢰도나 정보 유출 안전도가 정보 접근을 제어하는 효과적인 기준이 될 수 없음을 알 수 있다.

5.4.2 신뢰도 값이 편중된 경우(시나리오 2와 3)의 결과 분석

1) '거부'와 '허용'의 정확도

시나리오 2의 결과는 TidalTrust를 통해 계산된 신뢰도 값이 7 이상이므로 임계값이 7 미만일 때 접근이 거절된 경우가 존재하지 않는다는 점을 제외하면 접근이 거절된 경우와 접근이 허용된 경우의 정확도는 시나리오 1과 동일한 결과를 보인다.

2) '거부'와 '허용'의 재현율

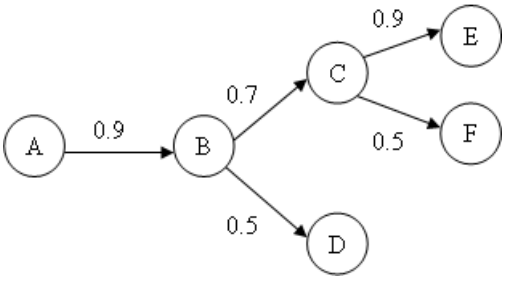
- α 값이 1일 때 접근이 거절된 경우의 재현율은 임계값이 7 이상일 때부터 계산되며 임계값이 10이 될 때까지 가파르게 상승한다.
- α 값이 0.5일 때 접근이 거절된 경우의 재현율은 임계값이 약 4일 때부터 계산되는 데, 이는 HTRS가 정보 유출 안전도 값에 의해 조정되었기 때문이다.
- 정보 접근이 허용된 경우의 재현율은 시나리오 1과 마찬가지로 정보 접근이 거부된 경우의 재현율과 반대의 패턴을 보인다.
- α 가 0.2인 경우의 재현율에 대한 그래프는 α 가 0.5인 경우에 비해 α 가 0 인 그래프에 더 가깝게 된다.

3) 결과에 대한 분석

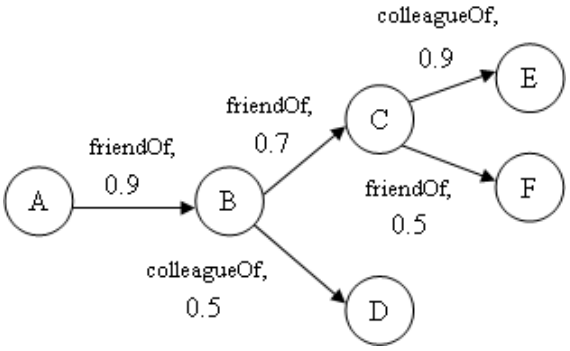
- (그림 13)에서 (그림 16)까지 8개의 그래프를 통해 편중된 분포의 신뢰도 값들에 있어 정보 유출 안전도가 효과적인 제어기로 동작함을 알 수 있다.
- 시나리오 2와 3의 결과는 각 사용자가 자신의 이웃에게 부여한 신뢰도 값들이 편중된 분포를 가질 때 α값이 접근제어의 재현율에 직접적인 영향을 끼침을 보여준다. 따라서 접근제어의 재현율 성능을 높이기 위해서는 최적의 α값을 찾는 것이 필요하다. 그런데 문제는 접근 '거절'과 '허용'의 재현율 값이 α값에 따라 서로 반대되는 패턴을 가진다는 것이다. α값이 커지면 '거절'의 재현율 값은 낮아지고 '허용'의 재현율 값은 높아지며, α값이 작아지면 '거절'의 재현율 값은 높아지고 '허용'의 재현율 값은 낮아진다. 다시 말해 HTRS의 계산에 있어 신뢰도 점수의 비중이 커지면 '거절'의 재현율 값은 낮아지고 '허용'의 재현율 값은 높아지며, 안전도 점수의 비중이 커지면 '거절'의 재현율 값은 높아지고 '허용'의 재현율 값은 낮아진다. 결론적으로 신뢰도 쪽에 비중을 두고 접근 제어를 하면 타인의 정보 접근을 최대로 허용해 줄 수 있으나 그만큼 정보가 유출된 가능성은 크며, 안전도 쪽에 비중을 두고 접근 제어를 하면 정보 유출의 가능성은 최소화될 수 있으나 타인과의 정보 공유에 지장을 받게 된다. 이러한 특성은 각 정보의 민감도에 따른 차등적인 접근제어에 이용될 수 있을 것이라 생각하며 이는 후속 연구에서 수행할 예정이다.

6. 관련 연구

D-FOAF[8]은 온라인 소셜 네트워크에서 접근 권한 위양(delegation)을 위해 친밀도 지표(friendship level metrics)와 거리에 기반을 둔 정책을 이용하는 방안을 제시하였다. (그림 17)은 간단한 소셜 네트워크를 나타내고 있다. 각 에지 위의 숫자는 친밀도 지표로 0부터 1까지의 값을 가진다. (1은 전적으로 신뢰하는 것을 의미한다.) 거리는 소스로부터 목적지까지의 최단 경로에 대해 소스 노드를 제외하고 목적지를 포함하는 노드의 개수로 정의된다. 예를 들어 사용자 B가 C에 대해 가지는 친밀도는 0.7이며, 사용자 A에서 F까지의 거리는 3이다. 또한 간접 연결 친밀도 지표는 최단 경로에 존재하는 모든 친밀도 값들을 곱한 값으로 정의된다.



(그림 17) 친밀도가 표시된 소셜 네트워크



(그림 18) 관계 타입과 신뢰도가 표시된 소셜 네트워크

예를 들어 사용자 A가 사용자 E에 대해 가지는 간접 연결 친밀도는 0.567이다. D-FOAF에서는 친밀도와 거리 값을 조절하여 사용자의 정보 접근을 제어한다. 예를 들어 접근을 허용하는 친밀도의 임계값을 0.5로 정의하였다면 사용자 A의 정보에 B (0.9), C (0.63), E (0.567)는 접근이 허용되나, D (0.45), F (0.315)는 접근이 거부된다. 또한 접근 허용 거리를 2로 정의하였다면, 사용자 A의 정보에 E와 F는 접근할 수 없다.

[7]은 온라인 소셜 네트워크를 위한 규칙 기반 접근 제어를 제시하고 있는 데, 기본적인 모델은 D-FOAF와 유사하나, 사용자 간의 관계가 타입을 가진다는 것과 거리를 깊이(depth)로 친밀도를 신뢰도(trust level)로 명명하는 점이 다르다. (그림 18)은 (그림 17)의 소셜 네트워크에 관계 타입이 추가된 경우이다 (원 논문에서는 화살표의 방향이 반대이다). 여기서는 간접 연결이 관계 타입에 의해 제약을 받을 수 있다. 예를 들어 A와 F 사이에는 간접 연결이 성립되지만, A와 E 사이에는 간접 연결이 성립되지 않는다. 뿐만 아니라 정책이 규칙 형태로 정의된다. 예를 들어 깊이 1에서 friendOf type을 가지면서 신뢰도가 0.7 이상이고, 거리 2에서 friendOf 타입을 가지면서 신뢰도가 0.6 이상인 간접 연결을 정의할 수 있다.

이러한 방식들은 관계의 속성인 타입, 거리, 신뢰도를 기반으로 한 접근 제어를 제공함으로써 소셜 네트워크의 특징을 반영하고 있다는 장점이 있다. 그러나 [8]의 경우 간접 연결에 대한 신뢰도 계산 방식이 적합하지 않다고 판단되며, [7]의 방식을 적용하려면 사용자가 일일이 규칙을 정의하는 것이 필요한 데, 이는 사용자에게 큰 부담으로 작용할 거라 생각한다. 본 논문에서 제안한 방식은 간접 연결의 신뢰도 계산에 잘 알려진 TidalTrust 알고리즘을 이용하였으며, 사용자는 접근 제어를 위해 신뢰도 임계값만 선택하면 되는 간단한 방식을 제공한다. 특히 접근제어의 기준이 되는 지표로 신뢰도와 정보 유출 위험도를 합성한 값을 이용함으로써 기존 접근제어 방식들과 차별화된 특성을 가진다.

7. 결론 및 향후 연구과제

향후 다양한 연구와 활용의 대상이 될 것으로 예상되는 온라인 소셜 네트워크에 있어 개인 정보 보호 장치를 마련하는 것은 반드시 필요하다. 현재 이러한 문제를 해결하기 위한 몇 가지 시도가 진행 중이나 전통적인 기밀성 보호 방식인 접근 제어 기법에 기반을 두고 있기 때문에 정당한 사용자에 의한 정보 유출 문제를 해결하지 못한다. 온라인 소셜 네트워크는 그 특성상 자신이 잘 알지 못하는 사람에게 정보 접근을 허용해야 할 필요가 있으므로 이를 고려한 적절한 해결책이 필요하다. 이에 본 논문에서는 사용자 간 신뢰도와 각 사용자의 정보 유출 위험도를 합성한 지표를 기반으로 접근 제어를 수행하는 방안을 제안하였다. 실험을 통해 직접 또는 간접 연결된 사용자의 정보 접근 제어에 있어 정보 유출 위험도가 중요한 역할을 담당할 수 있음을 알 수 있었다. 그러나 현재까지의 실험 방식과 결과가 본 논문이 제시한 접근 제어 방식이 가지는 실효성을 온전히 증명하지는 못한다고 생각하며 향후 지속적인 연구를 통해 검증 방법을 찾고자 한다.

정보 유출 위험도를 통해 부여되는 정보 유출 안전도 값은 특정 사용자가 직접 연결된 다른 사용자의 신뢰도 값을 부여하지 않은 경우나 간접 연결이 존재하지 않는 사용자의 경우에 정보 접근을 제어하기 위한 기준으로도 사용될 수 있다고 생각한다. 뿐만 아니라 각 한 개인의 공간에 존재하는 정보들이 상이한 민감도를 가지는 현실에서 민감도에 따른 차등적인 접근 허용을 적용함에 있어 정보 유출 안전도 값이 유용한 제어 기준으로 사용될 수 있다고 생각한다.

본 논문을 통해 신뢰도를 기반으로 하는 온라인 소셜 네트워크의 접근에 있어서 신뢰도 값의 분포 특성이 중요한 인자로 작용하는 것을 확인할 수 있었으며, 향후 이에 대한 추가적인 연구가 필요하다고 생각한다. 또한 본 논문에서 정보 유출 안전도 순위를 안전도 레벨로 변환할 때 단순한 방식을 사용하였는데, 이에 대한 추가적인 연구도 향후 진행할 예정이다.

참 고 문 헌

[1] E. Adar and C. Re, “Managing uncertainty in social networks,” IEEE Data Engineering Bulletin, 30 (2), pp.15-22, 2007.

[2] Stefan Weiss, “Online Social Networks and the Need for New Privacy Research in Information and Communication Technology,” Third International Summer School organized by IFIP WG 9.2, 9.6/117, 11.6, 6th-10th August, 2007, Sweden.

[3] Ralph Gross, Alessandro Acquisti, H. John Heinz III, “Information revelation and privacy in online social networks,” Proceedings of the 2005 ACM workshop on Privacy in the electronic society, November, 07-07, 2005, Alexandria, VA, USA

[4] Jianming He, Wesley W. Chu and Zhenyu (Victor) Liu, “Inferring Privacy Information from Social Networks,” Lecture Notes in Computer Science, Volume 3975, pp.154-

165, 2006.
[5] Wanhong Xu, Xi Zhou, Lei Li, “Inferring privacy information via social relations,” IEEE 24th International Conference on Data Engineering Workshop(ICDEW 2008), 525-530, 7-12 April, 2008.
[6] David Rosenblum, “What Anyone Can Know: The Privacy Risks of Social Networking Sites,” IEEE Security and Privacy, Vol.5 No.3, pp.40-49, May, 2007.
[7] B. Carminati, E. Ferrari and A. Perego, “Rule-based Access Control for Social Networks”, OTM Workshops, LNCS 4278, pp.1734-1744, 2006.
[8] Sebastian Ryszard Kruk , Sławomir Grzonkowski1, Adam Gzella1, Tomasz Woroniecki1, and Hee-Chul Choi, “D-FOAF: Distributed Identity Management with Access Rights Delegation,” LNCS 4186, pp.140-154, 2006.
[9] A. Sabelfeld and A. C. Myers, “Language-Based Information -Flow Security,” IEEE Journal on Selected Areas in Communications, 21, pp.5-19, 2003.
[10] Carrie Gates, “Access Control Requirements for Web 2.0 Security and Privacy,” W2SP 2007 (Web 2.0 Security & Privacy 2007).
[11] Michael Hart, Rob Johnson, and Amanda Stent, “More Content-Less Control: Access Control in the Web 2.0,” W2SP 2007 (Web 2.0 Security & Privacy 2007).
[12] Amin Tootoonchian, Kiran K. Gollu, Stefan Saroiu, Yashar Ganjali, and Alec Wolman, “Lockr: Social Access Control for Web 2.0,” First ACM SIGCOMM Workshop on Online Social Networks (WOSN), Seattle, WA, August, 2008.
[13] A. Josang, R. Ismail, C. Boyd, “A Survey of Trust and Reputation Systems for Online Service Provision,” Decision Support System, 2006.
[14] J. Golbeck and J. Hendler, “Accuracy of Metrics for Inferring Trust and Reputation in Semantic Web-based Social Networks,” Proceedings of the EKAW 2004, 2004.
[15] D. Gambetta, “Can we trust trust?,” In: D. Gambetta (ed.) Trust: Making and Breaking Cooperative Relations, pp.213-237, Oxford, 2000.
[16] P. Resnick and R. Zeckhauser, “Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system,” Technical report, University of Michigan, 2001.
[17] P. Resnick, R. Zeckhauser, J. Swanson and K. Lockwood, “The value of reputation on eBay: a controlled experiment,” Working Paper, 2002.
[18] Amy N. Langville and Carl D. Meyer, “Google's PageRank and Beyond: The Science of Search Engine Rankings”, Princeton University Press, July, 3, 2006.
[19] P. C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger, “Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control,” Technical report, IBM Research Report RC24190, 2007.
[20] C. Ziegler and George Lausen, “Propagation Models for Trust and Distrust in Social Networks”, Information Systems Frontiers, Vol.7 No.4-5, pp.337-358, December, 2005.
[21] L. Mui, M. Mohtashemi, and A. Halberstadt, “A Computational Model of Trust and Reputation”, Proceedings of the 35th Hawaii International Conferences on System Sciences, Big Island, HI, USA, pp.188-196, January, 2002.
[22] K. K. Bharadwaj, M. Y. H. Al-Shamri, “Fuzzy Computational Models for Trust and Reputation Systems”, Electronic Commerce Research and Applications, Volume 8, Issue 1, pp.37-47, January, 2009.
[23] L. Page, S. Brin, R. Motwani, T. Winograd, “The Pagerank Citation ranking: Bringing Order to the Web”, Technical Report, Stanford Digital Library Technologies Project, 1998.
[24] J. Golbeck, “Computing and Applying Trust in Web-Based Social Networks,” Ph.D. Dissertation, University of Maryland, College Park, 2005.

서 양 진

e-mail : yjseo@ec.cse.cau.ac.kr
1998년 중앙대학교 컴퓨터공학과(학사)
2000년 중앙대학교 컴퓨터공학과(석사)
2006년 중앙대학교 컴퓨터공학과(박사수료)
2002년~2003년 아시안사인(주) 전자거래연구원 팀장
2004년~현 재 소프트캠프(주) 정보보안기술연구소 팀장
관심분야 : 정보보안, 시맨틱 기술, 정보검색, 인공지능

한 상 용

e-mail : hansy@cau.ac.kr
1975년 서울대학교 공과대학(학사)
1984년 University of Minnesota(공학박사)
1984년~1995년 미국 IBM 연구소 책임연구원
1999년~2005년 JTC1/SC22-Korea 위원장
2005년~2006년 한국SW감정평가학회 회장
2006년~2008년 중앙대학교 정보통신연구원 원장
2007년~2009년 중앙대학교 정보대학원 원장
1995년~현 재 중앙대학교 컴퓨터공학부 교수
2005년~현 재 IJWSP 편집장
관심분야 : 차세대 웹 기술, 정보검색, 최적화