情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

소셜 네트워크 서비스에서의 동적 사용자 신뢰도 평가 스킴*

이 창 훈,† 정 영 만, 정 재 욱, 원 동 호‡
성균관대학교 정보보호연구소

Dynamic User Reliability Evaluation Scheme for Social Network Service*

Changhoon Lee,† Youngman Jung, Jaewook Jung, Dongho Won‡
Information Security Group, Sungkyunkwan University

요 약

소셜 네트워크 서비스는 생산자와 소비자의 구분 없이 모든 사용자가 직접 정보를 생산, 가공, 유통할 수 있는 양방향 미디어이다. 이용자 수가 빠르게 증가하면서 사용자들이 다양한 정보를 획득하고 공유할 수 있게 되었지만 서비스 상에서 신뢰할 수 없는 정보들의 확산으로 인한 문제점이 발생하고 있다. 또한, 개방적 환경이라는 점을 악용하여 사용자의 프라이버시를 침해하고 서비스 및 사용자의 신뢰도를 낮추는 문제가 확산되고 있다. 따라서 민감한 정보는 정보 생산자가 신뢰할 수 있는 사람에게만 전달될 수 있어야하고, 신뢰할 수 있는 사람으로부터 정보를 제공받아야한다. 이러한 필요성으로 인해 사용자의 신뢰도를 평가할 수 있는 효율적인 방법이 필요하다. 본 논문에서는 서비스에서의 신뢰를 정의하며, 서비스의 기능을 활용하여 Trust Parameter를 만들고 사용자의 신뢰도를 평가할 수 있는 동적 사용자 신뢰도 평가 스킴을 제안한다. 그리고 제안한 신뢰도 평가 스킴에 대한 분석을 통해 사용자들의 신뢰도에 대한 신뢰 범위를 도출한다.

ABSTRACT

The social network service is the bidirectional media that all of the users are be able to directly produce, process, and distribute the information without distinction of the producer and consumer. Over increasing the users rapidly, the users are be able to obtain and share the various information, but the problems occur due to the spread of unreliable information on the service. Moreover, it is spreading the problems violating the privacy and decreasing the reliability of the users by exploiting the open environment. Therefore, sensitive information can be delivered only to users which information producer can trust, and the users should get the information from the trustworthy users. Due to this necessity, it needs the efficient method can evaluates the reliability of the users. In this paper, we define the reliability in the service, make the trust parameter by using the function of the service, and propose the dynamic user reliability evaluation scheme evaluating the reliability of users. We draw the trust range on the reliability of users by analyzing the proposed reliability evaluation scheme.

Keywords: Social network service, Reliability evaluation, SNS security, Privacy protection

I. 서 론

최근 소셜 네트워크 서비스의 가입자 수가 빠르게 증가하고 정보를 공유하는 주요한 수단으로 부각되면서 사회적으로 소셜 네트워크 서비스에 대한 관심이 증가하고 있다. TV, 신문, 라디오 등과 같이 정보 생산자가 소비자에게 한 방향으로 정보를 전달하는 단방

접수일(2012년 11월 13일), 게재확정일(2012년 12월 24일)
* 본 연구는 방송통신위원회의 방송통신융합미디어원천기술 개발사업의 연구결과로 수행되었음. (KCA-2012-12-912-06-003)
† 주저자, clee@security.re.kr
‡ 교신저자, dhwon@security.re.kr

향 미디어와는 달리 소셜 네트워크 서비스는 생산자와 소비자의 구분 없이 모든 사용자가 직접 정보를 생산, 가공, 유통할 수 있는 양방향 미디어로써 정보의 생산 과정이 단순하고 주변 사람들과 공유가 편리하기 때문에 빠르게 확산되고 있다. 소셜 네트워크 서비스를 통해 일상을 공유하고 정보를 습득 및 교환하는 일이 일상화 되었고, 사용자가 증가하면서 집단지성을 이루어 다양한 목적으로 활용이 되고 있다. 스마트 기기의 보급의 확대로 인해 소셜 네트워크 서비스 사용자들은 모바일 기기를 통해 어디서든 서비스에 접근이 가능하기 때문에 가입자 수는 더욱 증가하고 사회적 영향력이 더 커질 것으로 예상된다.

소셜 네트워크 서비스가 정보 공유의 장이 되면서 다양한 정보를 획득하고 공유할 수 있는 장점과 더불어 신뢰할 수 없는 정보들의 확산으로 인한 문제점이 발생하고 있다. 정보 생산자가 불분명한 정보들이 많고 그런 정보들이 무분별하게 확산되기 때문에 사용자들은 서비스 상의 정보들의 신뢰성 여부를 판단하기가 힘들고 거짓 정보들로 인한 피해 사례가 계속적으로 발생하고 있다. 또한, 의도하지 않은 정보의 확산으로 인해 개인의 민감한 정보가 다수의 사람들에게 공유되어 프라이버시 침해가 발생하고, 온라인 환경이라는 점을 악용하여 신분을 위장하거나 다수의 계정을 만들어서 피해를 발생시키며 서비스의 신뢰도를 낮추는 문제가 확산되고 있다. 따라서 이러한 문제점에 대응하기 위해서는 정보의 생산자인 사용자 계정 즉, 노드에 대한 신뢰도를 평가할 필요성이 있다. 노드의 신뢰도에 따라 정보의 신뢰도를 판단할 수 있고, 거짓 정보에 대한 피해나 거짓 계정으로 인해 발생되는 위협을 예방할 수 있다. 이 노드의 신뢰도를 통해 서비스 사용자들은 정보의 신뢰성을 판단할 수 있는 기준이 확립되고, 민감한 정보를 공유하고자 할 때 노드의 신뢰도를 확인하여 선별적으로 공유할 수 있다. 정보 생산자가 정보를 공유하길 원하는 사람에게만 전달되고 정보를 확인할 수 있는 사람을 제한할 수 있도록 하는 것이 프라이버시 침해 피해를 최소화할 수 있는 방법이다.

하지만 프라이버시 침해 문제에 대한 대응 방안을 제안할 때 고려할 점은 소셜 네트워크 서비스의 주요한 특성인 개방성을 훼손하지 않아야 한다. 정보의 개방성으로 인해 소셜 네트워크 서비스가 빠르게 확산될 수 있었고, 이러한 개방성은 소셜 네트워크 서비스의 원동력이라 할 수 있다. 하지만 이러한 개방성으로 인해 프라이버시 침해 문제가 발생하고 있기 때문에 이 두 요소를 절충하는 방안이 필요하다. 개인이 정보를 공유할 때 공유하고 자하는 사람에 대한 필터링이 필요하고 그 척도는 신뢰라고 할 수 있다. 공개적인 정보는 누구나 확인해도 되지만 개인에게 민감한 정보는 정보 생산자가 신뢰할 수 있는 사람에게만 전달될 수 있어야한다.

이러한 필요성으로 인해 소셜 네트워크 서비스에서 노드의 신뢰도를 판단하기 위한 다양한 방법이 제안되었다. 하지만 지금까지의 연구들은 노드의 프로필 정보나 개인 정보를 기반으로 공통점을 추출하여 신뢰도를 평가 및 검증하는 방법들이 제안해왔고 신뢰라는 추상적인 개념을 구체화하여 소셜 네트워크 상에서 구현하는 방법은 아직까지 제안되지 않았다. 사람들 간의 신뢰는 고정적인 요소가 아닌 계속적으로 변하는 요소이며 유동성을 고려하여 신뢰도를 평가하는 동적 사용자 신뢰도 평가 스킴이 필요하다.

본 논문에서는 신뢰에 대한 정의를 제시하고, 그 정의와 소셜 네트워크 서비스 상에서 공통적으로 서비스되는 기능과의 매핑을 통해 소셜 네트워크 서비스 상에서도 현실에서 신뢰를 갖는 사람과의 관계를 표현할 수 있는 스킴을 제안한다. 본 논문의 구성은 다음과 같다. 2장 관련 연구에서는 소셜 네트워크 서비스의 정의와 보안 위협을 분석하고 기존 연구의 한계를 분석하며 신뢰도를 정의한다. 3장에서는 신뢰의 정의에 따른 파라미터들과 소셜 네트워크 서비스의 기능들과의 매핑을 통해 동적 사용자 신뢰도 평가 스킴을 제안한다. 4장에서는 실험 및 결과 분석, 5장에서는 본 논문에 대한 결론을 맺는다.

II. 관련 연구

2.1 소셜 네트워크 서비스의 정의와 보안 위협

소셜 네트워크 서비스는 사용자들의 관계성에 기반하여 정보를 생성 및 유통하는 서비스 모델이다. 서비스에서 제공하는 도구 및 환경을 이용하여 사용자는 스스로 쉽게 정보를 생성하고 자신이 속한 소셜 그룹에 공유가 가능하다. 그리고 그 정보에 대해 실시간으로 자유롭게 의견을 교환하고 정보를 수정 및 확산시킬 수 있다. 시간과 공간의 제약이 없고 자유로운 소통이 가능한 소셜 네트워크 서비스의 등장으로 인해 서비스 제공자 중심에서 소비자 중심으로 지식 정보의 생산 및 유통이 변화하고 있다. 소셜 네트워크 서비스에서 일반 사용자들은 일상을 다른 사람과 공유하거나

〔표 1〕 소셜 네트워크 서비스에서 보안위협

구분	보안 위협	내용
인증	신원 도난 공격	실제 사용자의 신원 정보를 악의적인 목적으로 획득하여 신원 정보의 주인으로 가장하여 활동하는 공격 형태
	시빌 공격	공격자가 다수의 신원 정보를 허위로 생성하고 이를 기반으로 평판을 조작하고 서비스의 신뢰도를 낮추는 공격
	평판 표백	서비스에 신규 가입하는 경우 주어지는 평판보다 낮은 평판이 주어지면 기존의 신원을 버리고 새로운 신원으로 시스템에 등록하는 악의적인 행동
프라이버시	인가 받지 않은 데이터 수집	각 사용자들의 프로필에 있는 정보들을 자동화된 소프트웨어로 수집하여 상업적인 목적이나 기타 악의적인 목적으로 사용하는 공격 형태
	프라이버시 블리칭	의도되지 않은 방법으로 프라이버시 침해가 이루어지는 형태의 공격으로 해당 소셜 네트워크 서비스에 공개한 정보가 관계를 맺은 다른 사용자에 의해 간접적으로 유포
기타	소셜 웹에서의 스팸	직접 스팸 데이터를 제작하여 유포하거나 타인이 생성한 스팸의 유포에 동참하는 공격 형태로 특정인이나 상표 또는 상품에 대한 과장된 내용 유포 및 긍정적 홍보나 부정적 이미지를 퍼트리는 등의 활동
	이클립스 공격	악의적인 의도를 가진 실제의 사용자들이 허위 사실을 유포하여 정상 사용자의 평판을 조작하고 서비스의 신뢰도를 낮추는 공격

최근 이슈가 되는 사실에 대해 의견을 개진하고 함께 실시간으로 토론하며, 관심사 및 취미 등에 관한 정보들을 획득하고 교환한다. 기업의 측면에서는 소비자들의 요구사항을 분석하고 기업을 알리기 위한 도구로 활용되고 있고, 정부기관의 측면에서는 국민의 목소리를 듣고 국민과의 소통을 위한 통로로 활용이 되고 있다.

그러나 소셜 네트워크 서비스의 이용자 수가 늘어나고 넓은 범위에서 활용되면서 보안 위협은 계속적으로 증가하고 있다. 소셜 네트워크 서비스의 개방적인 특성으로 인하여 서비스에 내재한 취약성들이 다수 존재하며 악의적인 공격자는 그 취약점을 악용하여 사용자와 서비스에 피해를 주고 신뢰도를 낮춘다. 사용자들의 프로필 정보 및 개인 정보들을 수집하고 서비스의 인증 취약점을 이용하여 새로운 계정을 만들어서 활동을 하거나 다수의 허위 계정을 생성하여 허위 사실을 유포하는 공격 형태가 발생할 수 있다. 또한 정보의 의도되지 않은 확산을 통해 프라이버시가 침해될 수 있는 위협이 있고, 수집된 데이터를 악용하여 스팸을 보내거나 다수의 사용자가 악의적인 의도를 갖고 허위 사실을 유포하여 신뢰도를 낮추는 공격을 할 수 있다. 〔표 1〕은 소셜 네트워크 서비스에서 발생할 수 있는 보안 위협을 나타낸다[2].

보안 위협들은 관계성에 따라 정보의 개방성을 추구하는 소셜 네트워크 서비스의 특성을 악용하여 사용자 및 서비스의 신뢰도를 낮춘다. 이러한 위협에 대응하기 위해 사용자 및 서비스가 노드의 신뢰도를 평가할 수 있는 지표가 필요하다.

2.2 기존 연구의 한계

소셜 네트워크 서비스의 프라이버시 보호 및 신뢰성 향상을 위한 연구들이 국내외에서 활발히 진행되고 있고 소셜 네트워크 서비스에 적용시키기 위한 프라이버시 보호 기술이나 신뢰도 평가 스킴들이 제안되고 있다. 하지만 기존 연구에서는 오프라인에서 사람사이의 신뢰한다고 느끼는 기준에 대한 정의가 명확하지가 않고, 프로필 정보 등의 고정적인 정보에 따라 노드들 사이의 공통점을 찾고 그 공통점을 분석하여 신뢰도를 판단하는 방법들이 제시되어왔다. 그 논문들의 목표는 관계성이 없는 사람과의 신뢰도를 계산하여 믿을 수 있는 사람인지 아닌지를 판단할 수 있는 기준을 제시하고 있다.

그러나 기존 연구의 한계는 프로필에 상호 관계된 요소가 있다는 것으로 신뢰할 수 있는 지에 대한 점이다. 예를 들어 같은 지역에 살고 있고 같은 학교를 졸업하여 같은 회사에 다니며 취미가 유사하여 같은 동호회에 가입되어 있는 사람이 있다고 할 때, 그 사람은 전혀 모르는 사람일 수도 있고, 행여나 알고 있는 사람이라고 하더라도 프로필에 있는 공통적인 요소가 때문에 신뢰한다고는 보장할 수 없을 것이다.

따라서 프라이버시를 보호하고 신뢰성을 판단하기 위해서는 고정적인 요소들을 사용한 정적인 신뢰도가 아니라 시간과 상황을 반영하는 동적인 신뢰도를 평가

해야할 필요성이 있다. 본 논문에서는 신뢰의 정의를 제시하고, 신뢰의 정의로부터 Trust Parameter를 도출한 후 이 Parameter를 소셜 네트워크 서비스의 기능에 매핑(Mapping)하여 동적으로 변화하는 사용자 신뢰도 평가 스킴을 제안한다. 제안된 스킴은 소셜 네트워크 서비스에서 사람들과 관계를 형성한 후에 시간과 상황의 변화를 계속적으로 반영하여 관계된 사람의 신뢰도를 판단할 수 있는 척도로 활용될 수 있을 것이다.

2.3 신뢰도의 정의

Francis Fukuyama 교수는 신뢰에 대해 "어떤 공동체내에서 그 공동체의 다른 구성원들이 보편적인 규범에 기초하여 규칙적이고 정직하며 협동적인 행동을 할 것이라는 기대"라고 정의하였다[3]. 즉, 사람에 대한 신뢰는 보편적인 규범과 규칙을 따르고 공통된 가치를 공유함으로써 발생하고 그런 행동이 규칙적이고 반복적으로 발생할 것이라는 기대라고 할 수 있다. 신뢰의 정의에 따라 사람을 신뢰한다고 생각하는 기준은 규범을 준수하고 공유된 가치의 방향성이 유사할 때 신뢰한다고 판단하며 그 가치를 공유하는 정도는 신뢰도에 영향을 미친다고 할 수 있다.

규범을 준수한다는 것은 주어진 환경과 조직에 잘 적응하는 사람을 뜻하고, 다른 사람에 대한 악의성이 없다는 것을 내포한다. 또한, 규범을 잘 준수하는 사람은 도덕적이고 윤리적일 것으로 기대하기 때문에 일반적으로 사람들은 규범을 잘 준수하는 사람을 신뢰한다.

공유된 가치의 방향성이 유사하다는 것은 서로의 생각이 유사하다는 것을 말한다. 협동적인 행동은 유사한 가치를 추구하고 동일한 목표와 목적을 설정하여 함께 행동한다는 것을 뜻한다. 사람들은 이질적인 사람보다는 유사한 가치를 갖고 동질감 있는 행동을 하는 사람을 더욱 신뢰하고 믿는다. 또한, 유사한 가치와 생각을 교류할 수 있기 때문에 사람 사이의 신뢰 관계를 형성하는데 중요한 요소가 될 수 있다.

교류의 정도는 관계 사이의 친밀감을 나타내며 이 지표는 보다 신뢰할 수 있는 지에 대한 검증 역할을 한다고 볼 수 있다. 교류의 정도는 규범의 준수 및 가치의 유사성과도 긴밀한 관계성을 갖고 있다. 보통 사람들은 정직하지 못하고 환경에 부적응하는 사람보다는 규범을 준수하고 정직한 사람과 친밀한 관계를 유지하길 원한다. 또한, 가치가 유사하고 생각이 비슷하면 빈번하게 정보를 공유하고 생각을 교류하면서 자연스럽게 친밀도가 증가하게 된다. 따라서 교류의 정도는 나머지 두 요소와 긴밀한 관계가 있고 친밀함은 두 요소에 대한 검증을 한다는 것을 뜻한다. 상호 간의 많은 교류를 할수록 친밀감은 올라가고 더불어 신뢰도도 비례하게 증가한다고 볼 수 있다.

실생활에서 사람과의 신뢰성에 대한 평가 정도와 교류 정도는 소셜 네트워크 서비스에서도 역시 본질적으로 유사하다. 따라서 이 기준을 소셜 네트워크 서비스의 기능에 매핑하여 동적인 사용자 신뢰도 평가 스킴을 구성할 수 있다.

III. 제안하는 동적 사용자 신뢰도 평가 스킴

3.1 Trust Parameter

제안 스킴에서 각 사용자 계정은 Node이고 신뢰도 평가를 받는 Node를 EN(Evaluated Node), 그리고 EN의 신뢰도를 확인하는 Node는 VN(Verifying Node)이라고 가정할 때 총 신뢰도(Total Reliability)는 공개신뢰도(Public Reliability)와 관계신뢰도(Relationship Reliability)로 구분한다. 공개신뢰도는 소셜 네트워크 서비스에서 EN이 관계를 맺고 있는 전체 Node의 집합에 대한 공개적인 신뢰도로 정의하고 P로 나타낸다. 관계신뢰도는 EN과 VN 이외의 모든 Node가 제외된 EN과 VN 사이의 개인적인 신뢰도 즉, 소셜 네트워크 서비스 상에서 개인과 개인 상호간의 신뢰도로 정하며 R로 표현한다. 여기서 공개신뢰도는 다수의 평가가 표현되기 때문에 객관성을 갖고 관계신뢰도는 개인과 개인 상호간의 평가이기 때문에 공개신뢰도에 비해 주관적인 성격을 갖는다.

공개신뢰도와 관계신뢰도를 구분한 이유는 VN이 EN의 신뢰도를 확인하는 상황이기 때문에 둘 사이의 신뢰도 평가 요소인 관계신뢰도를 사용하지만 단순히 EN과 VN 두 Node 사이의 가치 유사성과 교류 정도에 따라 평가를 하는 관계신뢰도만으로는 평가가 주관적일 수 있고 신뢰도 평가에서 오류를 범할 가능성이 크다. 그러므로 평가에 대한 객관성을 확보하기 위해 관계된 집단 전체의 의사를 반영할 필요성이 있기 때문에 공개신뢰도가 포함된다.

공개신뢰도와 관계신뢰도에는 신뢰도의 정의에 따라 세 가지의 Parameter로 구성된다.

첫 번째 Parameter는 규범준수정도(N)이다. 주

어진 시간동안 서비스 내에서 통념적인 규범을 잘 준수했는가에 대한 Parameter로써, 규범과 규칙을 준수하고 정직하다는 것은 경험적으로 판단이 가능하기 때문에 과거의 특정 시점부터 현재 시점까지의 시간(t) 동안 서비스의 규정과 규범을 충실히 따랐는지에 대한 수치이다. 서비스의 특성상 고려할 점은 소셜 네트워크 서비스의 개방성을 최소화해야하기 때문에 규범과 규칙을 따르는 것이 정보의 생산에 방해가 되어서는 안 된다. 어떤 사상이나 주관적인 생각이 지배해서는 안 되고, 객관적이고 통념적인 생각에 기인한 규범이어야 하기 때문에 이 규범과 규칙은 생각과 표현의 자유를 보장하되 타인을 비방하거나 명예를 훼손하고 피해를 주는 정보 등의 기본적인 예의에 어긋난 언행에 대한 것으로만 한정한다. 이 Parameter N과 매핑되는 서비스의 기능은 다른 사용자로부터의 관계 차단, 신고, 그리고 욕설 등의 부정적인 언어 사용으로 인한 필터링 등이 있다. 다른 사람에게 피해를 주는 말과 정보 등으로 인하여 타인으로부터 관계가 차단되거나 신고를 당하게 되면 사용자 및 서비스에 피해를 주는 행위를 했다고 판단하여 N 값이 감소한다. 단, 악의적인 사용자에 의한 고의적인 신고 및 차단을 방지하기 위해 해당 요소에 대하여 Node별 빈도수를 조사하여 특별히 높은 경우에는 제한을 하거나 경고를 하여 정상적으로 활용될 수 있도록 서비스 제공자가 환경을 제공해야한다. 또한, 욕설 등의 부정적인 언어를 했을 경우도 타인의 명예를 훼손하고 피해를 주는 행위라고 간주되어 역시 N 값이 감소한다. N 값은 모든 사람이 동일한 시간동안 규범을 준수했는지에 대한 수치이므로, 기본 값인 D를 기준으로 규범을 어겼을 시 점차 감소한다. Prameter N은 식 (1)과 같이 나타낸다.

$$N = D - \frac{1}{h}\sum_{k=1}^{h} n_k \tag{1}$$

규범준수정도는 공개신뢰도와 관계신뢰도에서 각각 N_p와 N_r로 표현된다. h값에 따라서 서비스의 기능 개수를 임의대로 조절할 수 있기 때문에 각 서비스 별로 적합한 기능을 추가하거나 제외시킬 수 있다.

두 번째 Parameter는 가치유사정도(V)이다. 공유한 글 및 정보에 대하여 다른 사용자들과 가치와 생각이 유사한지에 대한 Parameter로써, 이 수치는 유사한 가치를 띄고 동질감 있으며 공감이 가는 정보를 공유할 때 증가한다. Parameter V와 매핑되는 서비스의 기능은 추천, 스크랩(퍼오기), 그리고 동일한 그룹의 그룹원일 경우가 해당된다. 정보에 대하여 타인의 추천 및 스크랩 등의 상호작용이 있을 때 증가하고, 서비스에서 같은 그룹에 속해 있을 때도 V 값은 증가할 수 있다. Parameter V는 식 (2)와 같이 나타낸다.

$$V = \frac{1}{h}\sum_{k=1}^{h} v_k \tag{2}$$

가치유사정도는 공개신뢰도와 관계신뢰도에서 각각 V_p와 V_r로 표현된다.

세 번째 Parameter는 정보교류정도(F)이다. 상호 교류가 많다는 것은 친밀도가 높거나 필요성이 있기 때문인데 교류가 높게 되면 친밀도가 계속적으로 증가하고 정보를 공유함에 따라 상대방의 생각과 의도를 확인할 수 있는 수단이 될 수 있기 때문에 Parameter F는 신뢰도 평가에 영향을 준다. Parameter F와 매핑되는 서비스의 기능은 방문 횟수, 댓글, 메시지, 쪽지, 채팅 등이 있다. 이 요소들은 친밀도와 연관성이 있고, 친밀도가 증가할수록 신뢰도도 비례해서 증가한다. Parameter F는 식 (3)과 같이 나타낸다.

$$F = \frac{1}{h}\sum_{k=1}^{h} f_k \tag{3}$$

정보교류정도는 공개신뢰도와 관계신뢰도에서 각각 F_p와 F_r로 표현된다.

다양한 소셜 네트워크 서비스들에서 공통적으로 제공되는 기능들에 대해서 고려할 때, Trust Parameter와 서비스의 기능 매핑에 대한 테이블은 〔표 2〕와 같다.

〔표 2〕 Trust Parameter와 서비스의 기능 매핑 테이블

Trust Parameter	소셜 네트워크 서비스의 기능
규범준수정도(N)	관계 차단(n_1), 신고(n_2), 욕설 필터링(n_3)
가치유사정도(V)	추천(v_1), 스크랩(v_2), 동일 그룹(v_3)
정보교류정도(F)	방문 횟수(f_1), 댓글(f_2), 메시지(f_3), 쪽지(f_4), 채팅(f_5)

3.2 동적 사용자 신뢰도 평가 스킴

Trust Parameter들은 서비스 이용 시간과 활용 정도에 따라 계속적으로 값이 변하기 때문에 이 Parameter를 이용하여 소셜 네트워크 서비스에서 각 Node의 신뢰도를 평가할 수 있는 동적 사용자 신뢰도 평가 스킴을 구현할 수 있다.

공개신뢰도 P는 EN과 관계를 맺은 Node들이 평가하는 EN의 평균 신뢰도를 나타내므로 EN과 관계를 맺고 있는 전체 Node들의 수를 n이라고 할 때, 공개신뢰도 P는 각 Node들의 신뢰도의 합으로 표현할 수 있다. 따라서 공개신뢰도는 식 (4)와 같이 계산할 수 있다.

$$P=\frac{1}{n}\sum_{k=1}^{n}P_k \tag{4}$$

P_k는 EN과 관계를 맺은 Node들 각각의 신뢰도이다. 그리고 P_k는 식 (5)와 같이 나타낸다.

$$P_k=a_pN_{pk}+b_pV_{pk}+c_pF_{pk} \tag{5}$$

P_k는 Trust Parameter들의 합으로 계산될 수 있고, 식 (5)에서 a_p, b_p, c_p는 공개신뢰도에서 각 Trust Parameter에 대한 가중치를 나타내는 상수이다. 규범계수 a_p, 유사계수 b_p, 교류계수 c_p로 나타낸다. 식 (4)와 식 (5)에 의해 공개신뢰도 P는 식 (6)과 같이 나타낼 수 있다.

$$P=\frac{1}{n}\sum_{k=1}^{n}(a_pN_{pk}+b_pV_{pk}+c_pF_{pk}) \tag{6}$$

〔표 3〕 기호 설명

기 호	설 명
T	총 신뢰도
P	공개신뢰도
R	관계신뢰도
N_p / N_r	규범준수정도 (공개/관계)
V_p / V_r	가치유사정도 (공개/관계)
F_p / F_r	정보교류정도 (공개/관계)
a_p / a_r	규범계수 (공개/관계)
b_p / b_r	유사계수 (공개/관계)
c_p / c_r	교류계수 (공개/관계)
m_p	공개신뢰도의 가중치
n_r	관계신뢰도의 가중치

관계신뢰도 R은 EN을 평가하는 VN의 주관적 신뢰도이므로, 식 (5)에서 Node의 신뢰도를 표현하는 방식과 유사하게 식 (7)과 같이 나타낼 수 있다.

$$R=a_rN_r+b_rV_r+c_rF_r \tag{7}$$

관계신뢰도 R은 Trust Parameter들의 합으로 계산될 수 있고, 식 (7)에서 a_r, b_r, c_r은 관계신뢰도에서 Trust Parameter에 대한 가중치로써 규범계수 a_r, 유사계수 b_r, 교류계수 c_r로 나타낸다.

VN이 평가하는 EN의 신뢰도는 총 신뢰도(T)이다. 공개 신뢰도 P 값과 관계신뢰도 R 값을 이용하여 VN이 평가하는 EN의 총 신뢰도 값을 도출해 낼 수 있다. 총 신뢰도는 식 (8)로 나타낸다.

$$T=\sqrt{(m_pP)^2+(n_rR)^2} \tag{8}$$

식 (8)의 m_p과 n_r은 공개신뢰도와 관계신뢰도에 대한 가중치를 나타내는 비례상수로서 m_p은 공개신뢰도의 가중치, n_r은 관계신뢰도의 가중치를 나타낸다. 식 (8)에서의 m_p과 n_r의 값은 두 값이 변하더라도 총 신뢰도 값 평균의 일관성을 유지하기 위해 $m_p^2+n_r^2=1$을 만족하는 값이어야 한다. 따라서 m_p과 n_r값은 식 (9)와 같다.

$$m_p=\cos\theta, n_r=\sin\theta \tag{9}$$
(단, m_p와 n_r은 양수이고, $0\le\theta\le 90$)

m_p과 n_r값을 변경함으로써 공개신뢰도와 관계신뢰도의 비중을 조절할 수 있다.

IV. 실험 및 결과 분석

4.1 실험 환경 구성

본 논문에서 제안한 동적 사용자 신뢰도 평가 스킴에 대한 유효성을 판단하기 위해 소셜 네트워크 서비스의 관계성을 나타내는 환경을 구성하여 실험을 하였다. 실험 표본으로 200개의 Node를 생성하고, 각 Node들은 동일하게 20개의 Node들과 상호 관계(n = 20)를 형성한다. 각 Node들은 관계를 형성하고 있는 20개의 Node들에 대해서 서비스 기능별 수치를 일정한 범위 내에서 자동화된 랜덤 함수를 사용하여

〔표 4〕 서비스 기능별 입력 범위

Trust Parameter	서비스 기능	입력 범위		계수 값(a, b, c)
		최소 값	최대 값	
규범준수정도(N)	관계 차단(n_1)	0	0	4
	신고(n_2)	0	2	
	욕설 필터링(n_3)	0	5	
가치유사정도(V)	추천(v_1)	0	20	4
	스크랩(v_2)	0	20	
	동일 그룹(v_3)	0	2	
정보교류정도(F)	방문횟수(f_1)	0	100	2
	댓글(f_2)	0	50	
	메시지(f_3)	0	30	
	쪽지(f_4)	0	20	
	채팅(f_5)	0	30	

임의의 숫자를 선정한다. 그 기능별 수치는 〔표 2〕를 따라서 11개의 기능에 대한 수치로 한정한다. 각 기능별 수치에 대한 입력 범위는 〔표 4〕와 같다.

〔표 4〕는 일정 시간(t)동안 정상적인 사용자에 대한 입력 범위를 나타낸 것으로 정상 사용자는 대부분 규범을 준수하기 때문에 부정적인 사용에 대한 Parameter인 N의 입력 범위를 다른 Parameter에 비해 작게 설정을 하였다. 반면에 정상 사용자들이 서비스에서 제공되는 순방향 기능들에 대해서 빈번하게 사용을 하는 것으로 가정을 하고 V와 F의 기능들에 대한 입력 범위를 비교적 크게 두었다.

Trust Parameter의 계수 값들에 대한 설정은 계수 값의 합을 10을 기준으로 각 계수의 크기를 분배할 수 있고, 실험에서는 서비스의 기능 수준과 비중을 고려하여 규범계수와 유사계수를 교류계수보다 비교적 크게 설정을 하였다.

4.2 공개신뢰도 분석

각 Node의 공개신뢰도는 〔표 4〕의 입력 범위 내에서 각 기능 별 수치를 임의로 입력하고 각 Node와 관계된 Node들의 Trust Parameter를 식 (1),(2),(3)을 이용하여 계산한다. 각 Node들에 대한 Trust Parameter N_p, V_p, F_p 값을 계산한 후, 식 (5)를 이용하여 P_k값을 구한다(D=10이라 가정). 식 (6)을 이용하여 각 Node의 공개신뢰도 P를 구한다. 실험을 위해 생성된 200개 Node의 공개신뢰도 값은 〔그림 1〕과 같이 분포한다.

〔그림 1〕을 확인해보면 표본 200개 Node의 공개신뢰도 값은 평균은 109.25이고, 최소 값 90.5, 최대 값 123.35, 표준편차 4.38 값이 나온다는 것을 확인할 수 있다. 모든 Node는 정상적인 Node이므로 해당 값의 범위는 정상 Node에 대한 공개신뢰도 값의 범위라고 할 수 있다. 이 값의 범위가 정상 Node의 신뢰할 수 있는 값의 범위라고 할 수 있다.

정확한 신뢰 범위를 도출하기 위해 기능별 수치를 입력 범위 내에서 계속적으로 변화시키면서 수차례 랜덤하게 입력하여 평균을 계산하였고 그 평균값을 통해 더욱 신뢰성 있는 공개 신뢰도의 값의 범위를 확률적으로 도출해 낼 수 있었다. 도출한 공개신뢰도 값의 범위는 〔표 5〕와 같다.

반복된 실험에서 전체 Node의 공개신뢰도 평균은 109.3±0.5 이내의 값이 나온다는 것을 확인할 수 있었다. 〔표 5〕의 결과를 통해 공개신뢰도의 최대 및 최소 한계치에 대한 확률을 확인할 수 있다. 공개신뢰도 범위의 한계치를 이용하면 공개신뢰도의 값의 범위에 대한 확률을 구할 수 있고, 신뢰성 있는 값의 범위를

〔표 5〕 공개신뢰도 값의 범위에 대한 Node 분포 확률

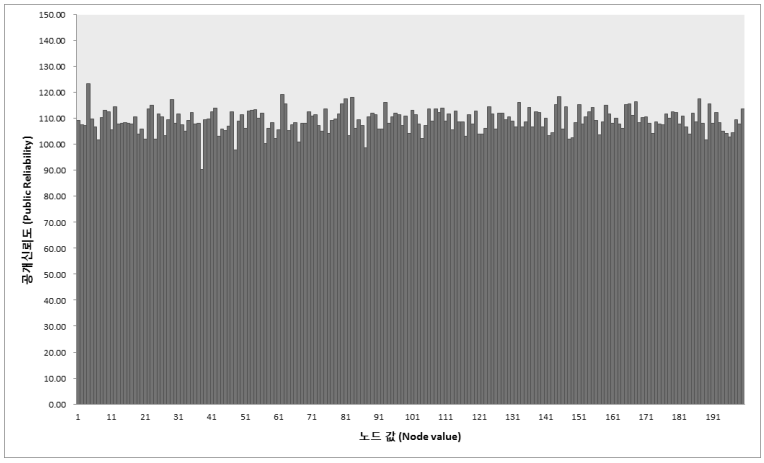
최대 한계치		최소 한계치	
한계치(이하)	확률(%)	한계치(이상)	확률(%)
122	99.9	106	78.53
121	99.75	105	85.1
120	99.47	104	89.82
119	99.02	103	93.48
118	98.33	102	95.87
117	96.78	101	97.7
116	94.80	100	98.77
115	91.65	99	99.25
114	86.95	98	99.6
113	81.45	97	99.88
112	73.95	96	99.92

도출할 수 있다. 소셜 네트워크 서비스에서 공개신뢰도의 범위에 따른 확률을 도출함으로써 정상 사용자들의 공개 신뢰도 값의 범위를 추정할 수 있는 근거를 마련할 수 있고, Node들의 객관성 있는 신뢰도 값을 도출하여 Node의 신뢰성을 평가할 수 있다.

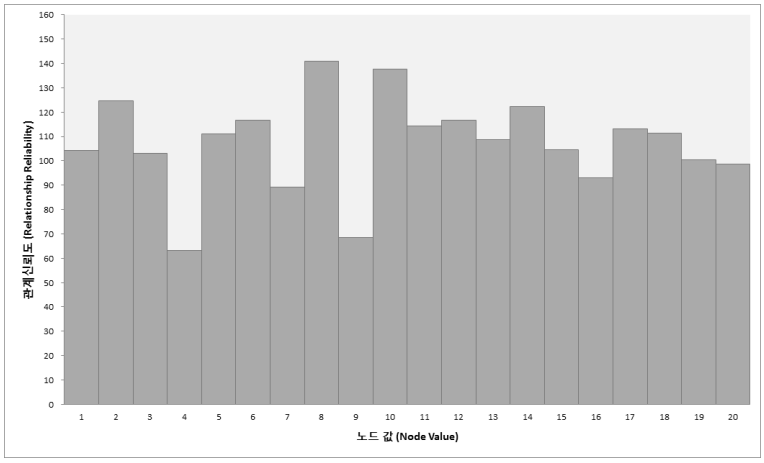
4.3 관계신뢰도 분석

관계신뢰도는 한 Node에 관계된 주변 Node들에 대한 주관적인 신뢰도이므로, 표본 200개의 Node 중에서 하나의 Node를 선정하여 그 Node와 관련된 20개의 노드에 대한 관계신뢰도를 분석하였다. 관계신뢰도는 식 (7)을 이용하여 계산할 수 있다. 실험에서 선정한 한 개 Node와 관계되어 있는 20개의 관계신뢰도는 〔그림 2〕와 같다.

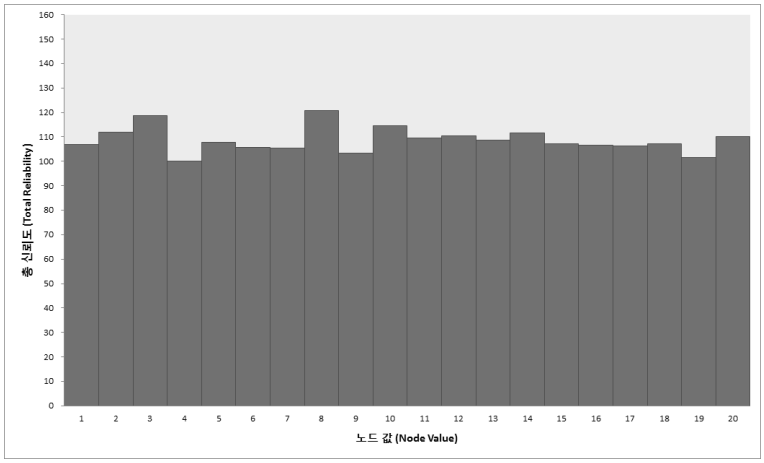
관계신뢰도는 한 Node와 연결되어 있는 Node들에 대한 주관적인 신뢰도 값이므로 공개신뢰도처럼 신뢰도 값의 범위에 대해 고려하는 것은 의미가 없다. 주관성이 짙기 때문에 공개신뢰도보다 편차가 상당히 크다는 것을 확인할 수 있다. 〔그림 2〕에서 분석한 관계신뢰도 값은 관계신뢰도의 평균은 107.08, 최대값 140.80, 최소값 63.07, 표준편차 19.22 값이 도출되었으며, 이 분포의 편차는 공개신뢰도의 편차보다 상당히 크다는 것을 볼 수 있다.



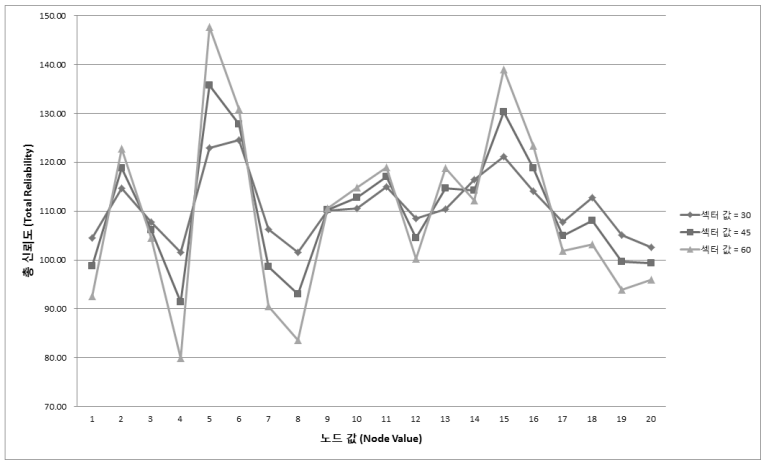
〔그림 1〕 Node별 공개신뢰도 값



〔그림 2〕 Node별 관계신뢰도 값



〔그림 3〕 Node별 총 신뢰도 값



〔그림 4〕 섹터 값에 따른 Node별 총 신뢰도 분포

4.4 총 신뢰도 분석

VN이 EN의 신뢰도를 평가하는 최종적인 목표 값은 총 신뢰도이고, 총 신뢰도는 공개신뢰도와 관계신뢰도를 이용하여 식 (8)을 계산하여 구할 수 있다. 식 (8)에서 총 신뢰도를 계산할 때, 객관성에 대한 비중을 더 고려하여 섹터 $\theta = 30$을 적용하였고, 이 θ값에 대한 신뢰도 가중치 값은 $m_p = 0.866$, $n_r = 0.5$이 된다.

관계 신뢰도 분석에서 평가한 Node들에 대한 총 신뢰도 값은 〔그림 3〕과 같다. 총 신뢰도 값은 VN을 선정하고 VN과 관계된 전체 Node를 평가한 값에 대해 분석한 값으로, 평가를 받는 각 EN의 공개신뢰도 분석 값과 관계신뢰도 분석 값을 식 (8)에 적용하여 값을 도출하였다. 〔그림 3〕에서 분석한 값은 총 신뢰도의 평균 108.70, 최대값 120.68, 최소값 100.14, 표준편차 5.09로써 편차가 작게 나타난다는 것을 확인할 수 있다. 편차가 작기 때문에 신뢰할 수 있는 신뢰도 범위를 측정하기 수월하고, 도출한 신뢰 범위는 범위 밖에 있는 Node들에 대해서는 특별 관리를 할 수 있는 근거가 될 수 있다. 총 신뢰도 값이 신뢰 범위보다 큰 Node는 특별히 강한 신뢰를 갖는 Node라고 판단할 수 있고, 신뢰 범위보다 작은 Node에 대해서는 평가자가 해당 Node의 신뢰성을 의심해볼 수 있다.

각 신뢰도의 가중치에 따른 총 신뢰도의 변화를 확인하기 위해 섹터 θ값을 변경하여 실험을 진행했다. 실험의 데이터는 〔그림 4〕와 같다. 섹터 θ값이 30, 45, 60에 대한 총 신뢰도의 분포이고, θ값이 작을수

록 공개신뢰도의 비중이 커지기 때문에 신뢰도의 편차가 작으며, θ값이 클수록 관계신뢰도의 비중이 커지기 때문에 신뢰도의 편차가 커지게 된다. 따라서 VN은 θ값을 조절함으로써 EN의 신뢰도에 대한 객관적인 데이터와 주관적인 데이터를 도출할 수 있고, 확률적으로 신뢰 범위를 구할 수 있다.

V. 결 론

소셜 네트워크 서비스는 개방성과 편리한 공유 기능 덕분에 전 세계적으로 빠른 시간에 확산될 수 있었고, 개방성은 소셜 네트워크 서비스의 주요한 특징이고 원동력이라고 할 수 있다. 하지만 개방성으로 인한 개인의 프라이버시 침해 사고가 계속적으로 발생되고 있기 때문에 개방성을 최대한 보장하고 개인 프라이버시 침해를 최소화 하는 것이 큰 과제로 남아 있다.

본 논문에서 제안한 동적 사용자 신뢰도 평가 스킴은 실생활에서 통용되는 신뢰에 대한 개념을 소셜 네트워크 서비스 내에서도 그대로 구현을 하기 위해 제안되었다. 제안된 스킴은 소셜 네트워크 서비스 상에서 관계된 사람과의 신뢰도를 평가할 수 있는 지표로 활용될 수 있으며, 상호간의 신뢰도는 계속적으로 변하기 때문에 신뢰도 값이 고정적이지 않고 관계의 변화를 반영하여 신뢰도가 변화하는 동적 스킴이라고 할 수 있다. 또한, 소셜 네트워크 서비스의 종류에 따라 제안 스킴의 기능 요소를 유동적으로 변경할 수 있기 때문에 어떤 소셜 네트워크 서비스에서도 적용할 수 있다.

사용자의 개인 성향에 따라 각 Parameter 및 공개신뢰도와 관계신뢰도에 대한 가중치를 설정할 수 있기 때문에 사용자 중심 평가 스킴으로써 활용될 수 있다.

따라서 제안된 스킴은 각 Node 신뢰도의 의미 있는 통계적 분석을 지원함으로써 소셜 네트워크 서비스에서 개인 프라이버시 보호 및 접근 제어를 위해 타인의 신뢰도를 평가할 수 있는 지표로 활용될 수 있을 것이다. 또한, 소셜 네트워크 서비스 사용자들의 신뢰도를 측정함으로써 사람들은 규범을 준수하고 소통을 원활히 하려고 노력하게 되고 이에 따라 바람직한 서비스 환경이 정착되어 그린 SNS 환경을 만드는데 기여할 것이다.

참고문헌

〔1〕 Hanjae Jeong, Changbin Lee, Jin Kwak, Dongho Won, Changyoung Kwon and Seungjoo Kim, "Privacy-enhanced social network service (SNS)," The 2011 FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing, Dec. 2011.

〔2〕 윤택영, 홍도원, "소셜 네트워크 서비스 신뢰성 강화 기술 동향," 전자통신동향분석, 26(4), pp. 134-145, 2011년 8월.

〔3〕 Muthucumaru Maheswaran, Hong Cheong Tang, and Ahmad Ghunaim, "Towards a Gravity-Based Trust Model for Social Networking Systems," 27th International Conference on Distributed Computing Systems Workshops(ICDCSW'07), pp. 24-31, Jun. 2007.

〔4〕 Francis Fukuyama, Trust : The social virtues and the creation of prosperity, Free Press Paperbacks, 1230 Avenue of the Americas New York, Jun. 1996.

〔5〕 윤택영, 홍도원, "소셜 네트워크 서비스에서 사용자 연락정보 프라이버시 강화를 위한 개인 프로필 관리 시스템 연구," 정보보호학회 논문지, 21(5), pp. 141-148, 2011년 10월.

〔6〕 Bimal viswanath, Ansley Post, Krishna P. Gummadi and Alan Mislove, "An Analysis of Social Network-Based Sybil Defenses," Proceedings of the ACM SIGCOMM 2010 Conference, pp. 363-374, Aug. 2010.

〔7〕 Anna Squicciarini, Federica Paci and Smitha Sundareswaran, "PriMa : An Effective Privacy Protection Mechanism for Social Networks," Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 320-323, Apr. 2010.

〔8〕 Wei Wei, Fengyuan Xu, Chiu C. Tan and Qun Li, "SybilDefender: Defend Against Sybil Attacks in Large Social Networks," 2012 Proceedings IEEE INFOCOM, pp.

1951-1959, Mar. 2012.
〔9〕 Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons and Abraham Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks," Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 267-278, Sep. 2006.
〔10〕 Sonja Buchegger, Doris Schioberg, Le-Hung Vu and Anwitaman Datta, "PeerSoN: P2P Social Networking: Early Experiences and Insights," Proceedings of the Second ACM EuroSys Workshop on Social Network Systems, pp. 46-52, Mar. 2009.
〔11〕 Jeawook Jung, Hakhyun Kim, Jaesung You, Changbin Lee, Seungjoo Kim and Dongho Won, "Construction of a Privacy Preserving Mobile Social Networking Service," Proceedings of IT Convergence and Services 2011, pp. 251-261, Oct. 2011.
〔12〕 성기훈, 공희경, 김태한, "AHP를 이용한 SNS 정보보호 위협요인 분석," 정보보호학회논문지, 20(6), 2010년 12월.
〔13〕 Weimin Luo, Jingbo Liu, Jing Liu and Chengyu Fan, "An Analysis of Security in Social Networks," 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 648-651, Dec. 2009.
〔14〕 Donghee Shin, "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption," Interacting with Computers, vol. 22, no. 5, pp. 428-438, Sep. 2010.
〔15〕 Hanjae Jeong, "Hash-based Key Management Architectures for Social Networks Services," Ph.D. Thesis, Sungkyunkwan University, Apr. 2011.
〔16〕 Maha Faisal and Asmaa Alsumait, "Social Network Privacy and Trust Concerns," Proceedings of the 13th International Conference on Information Integration and Web-based Applications and Services, pp. 416-419, Dec. 2011.

〈著者紹介〉

이 창 훈 (Changhoon Lee) 학생회원
2009년 2월: 성균관대학교 전자전기공학과 졸업
2012년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 암호학, 네트워크보안, 하드웨어보안, 역공학

정 영 만 (Youngman Jung) 학생회원
2012년 2월: 성균관대학교 수학과 졸업
2012년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 암호이론

정 재 욱 (Jaewook Jung) 학생회원
2010년 2월: 한국항공대학교 전자전기컴퓨터공학과 졸업
2012년 2월: 성균관대학교 전자전기컴퓨터공학과 석사
2012년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 박사과정
〈관심분야〉 정보보호, 암호학, 네트워크 보안, 포렌식

원 동 호 (Dongho Won) 종신회원
1976년~1988년: 성균관대학교 전자공학과(공학사, 공학석사, 공학박사)
1978년~1980년: 한국전자통신연구원 전임연구원
1985년~1986년: 일본 동경공업대 객원연구원
1988년~2003년: 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
현재: 성균관대학교 전자전기컴퓨터공학과 교수, 한국정보보호학회 명예회장
〈관심분야〉 정보보호, 암호이론, 정보이론