소셜 네트워크에서 안전한 데이터 공유를 위한 애드혹 네트워크 키 관리 기법

김가린° 홍충선
경희대학교
grkim@networking.khu.ac.kr, cshong@khu.ac.kr

Ad hoc network Key Management Mechanism for Secure Data Sharing in Social Network

Ga Rin Kim° Choong Seon Hong
Kyung Hee University

요 약

최근 빠르게 확산되고 있는 소셜 네트워크 서비스(Social Network Service)는 사용자 간 데이터의 공유 및 전파, 그리고 가상의 공간을 이용한 지인과의 인맥 관리와 새로운 인맥 생성에 널리 사용되고 있다. 그러나 소셜 네트워크의 공개적인 환경에 의해 정보나 프라이버시가 쉽게 노출될 수 있다. 특정 정보를 가진 사용자들 간의 제한적 정보 공유는 소셜 네트워크의 이러한 단점을 완화시킬 수 있을 뿐만 아니라 사용자가 원하는 정보를 가진 다른 사람들과의 정보공유를 통해 정보에 대한 신뢰도를 높이며, 새로운 인맥 형성에도 효과적 일 것이다. 본 논문에서는 이러한 소셜 네트워크에서 동일한 관심사를 가진 사용자들 간의 폐쇄적 정보공유에서의 정보 보호와 악의적 사용자에 의한 도청을 막기 위한 데이터 암호화 메커니즘을 제안한다.

1. 서론

인터넷 및 네트워크를 이용한 정보의 공유 및 확산, 그리고 인맥 관리 및 생성을 위한 소셜 네트워크가 빠르게 확산되고 있다.[1] 그러나 소셜 네트워크 환경에서는 매우 공개적으로 정보를 공유하여 개인이 공개한 정보들로 인해 개인정보가 쉽게 노출 될 수 있으며 공개된 정보는 다른 사용자들에 의해 무분별하게 전파될 수 있는 단점이 있다.[1] 또한 악의적 사용자에게 정보가 쉽게 노출되며 도청에 의해 피해를 받을 수 있다.

이러한 문제점을 해결하기 위해 동일한 관심사를 가진 사용자들 간의 제한된 네트워크를 생성하고 고유한 그룹키를 이용해 정보를 전송함으로써 정보를 보호할 수 있는 메커니즘이 필요하다. 본 논문에서는 동일한 관심사를 가진 사용자들의 그룹을 생성하고, 무선 통신의 물리계층의 특성을 이용하여 생성한 그룹키를 이용하여 정보를 공유하는 메커니즘을 제안한다.

2. 관련 연구

무선으로 통신은 브로드캐스팅한 특징으로 인해 한 노드가 여러 노드에게 같은 정보를 전달하더라도 지연확산(Delay spread)으로 인해 정보를 전달받은 각각의 노드는 서로 다른 신호의 정보를 수신한다[2].

이러한 신호 정보를 이용하여 [3]에서는 무선 센서 노드 간 키 공유기법을 제안하고 있다. [3]에서는 두 센서 노드가 [2]에서 제안한 특성으로 공유하기 위해서는 센서 노드 사이에 있는 환경에 의한 신호의 세기나 주파수에 따라 다른 감쇄 현상을 보완할 방법을 제안하였다. 이러한 키 공유기법을 이용하여 두 노드사이의 안전한 통신이 이루어 질 수 있다.

본 연구는 방송통신위원회의 차세대통신네트워크원천기술개발사업의 연구결과로 수행되었음 (KCA-2011-08913-05002).
Dr. CS Hong is the corresponding author.

3. 제안사항

본 절에서는 그룹 내에서의 안전한 정보공유를 위한 정보 암호화 메커니즘을 제안한다. 제안된 메커니즘은 아래와 같은 사항들을 전제로 한다.

- 그룹 내의 모든 사용자와 그룹에 추가되는 모든 사용자는 신뢰할 수 있다.
- 모든 사용자는 2.2에서 소개된 기법을 통해 각 노드 간의 고유한 키를 생성 할 수 있다.
- 하나의 관심사로 만들어지는 그룹은 유일한 것으로 가정한다.
- 모든 사용자는 에드혹 네트워크를 구성하여 통신한다.

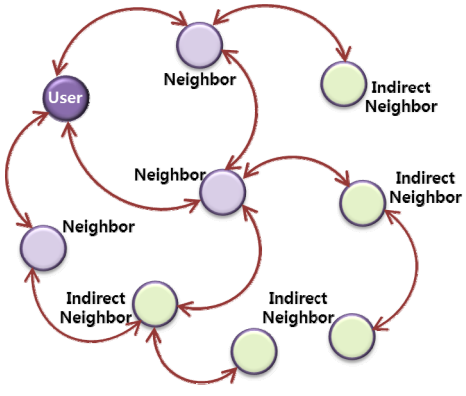

그림 1 소셜 네트워크의 구조

그림 1과 같이 소셜 네트워크 내의 모든 사용자는 1인 커뮤니티의 형태이며 각 사용자는 공개적으로 또는 인맥 관계에 놓인 사용자들 사이에서 정보를 공유할 수 있다. 또한 인맥관계에 있지 않더라도 여러 인맥을 거쳐 다른 사용자의 정보를 간접적으로 얻을 수 있다. 그러므로 사용자가 공개한 정보는 무분별하게 확장 및 배포 될 수

있으며 악의적 사용자에 의한 정보 도청이 발생 할 수 있다.

각 사용자의 관심사를 기준으로 소셜 네트워크 안에서 새로운 그룹을 생성 한다면 공통된 관심사를 가진 사용자간의 안전한 정보 공유가 가능해 짐으로서 정보의 무분별한 배포를 막을 수 있을 뿐 아니라 자신이 원하는 정보만을 공유하며 일반적은인 경우보다 양질의 정보를 얻을 수 있다. 또한 그룹키를 이용한 제한적 통신을 통해 악의적인 노드로부터 정보를 보호 받을 수 있다.

이러한 그룹키 생성 및 배포는 다음의 순서를 따른다.

(1) 관심사 확인요청 : 특정 관심사를 가진 '사용자A' 는 자신의 모든 이웃들에게 특정 관심사를 가지고 있는가에 대한 확인요청 메시지를 보낸다.

(2) *관심사 확인응답* : 확인요청 메시지를 전달받은 이웃 노드인 '사용자B' 는 자신의 관심사 중 해당 관심사와 같은 것이 있는지 확인하다. 만약 동일한 관심사가 있다면, 응답 메시지를 통해 자신이 해당 관심사를 가지고 있음을 알린다. 이때 무선 통신에서의 물리적 특성을 이용하여 두 사용자는 두 사용자 사이의 고유한 값 S_{AB}를 알 수 있다.

(3) *그룹키 생성* : '사용자A'는 (2)의 과정에서 탐색된 자신과 같은 관심사를 가지는 n개의 이웃 사용자와 각각의 고유한 값을 가지게 되며, 이러한 고유 값을 이용하여 그룹 내의 그룹키 G를 생성한다.

(4) *관심사 그룹 생성* :사용자A는 (2)의 과정에서 얻어진 각 노드와의 고유한 값을 이용하여 그룹키 G를 암호화한 후 해당 노드에게 전송하여 그룹키를 공유한다. 이를 통해 사용자 A와 사용자A와 같은 관심사를 가진 이웃노드들은 새로운 그룹을 형성하게 된다.

(5) *관심사 그룹멤버 추가* : 그룹키를 전달받은 이웃노드들은 자신의 이웃노드들 사이에 해당 관심사를 가지는 사용자를 알아낸다. 그 후 탐색된 이웃 노드에게 자신이 알고 있는 그룹키 G를 해당 이웃노드와의 고유값을 이용하여 암호화한 후 전송함으로서 해당 사용자를 그룹에 추가한다. (5)의 과정을 반복함으로서 새로운 사용자들을 그룹에 추가하여 그룹의 크기를 증가시킨다.

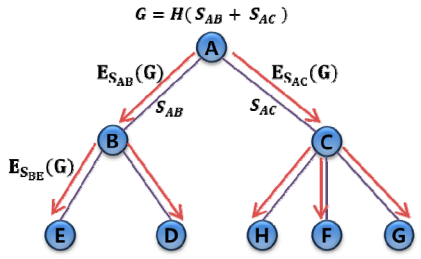

그림 2 그룹키 생성

표 1 사용된 기호의 의미

기호	의미
$H(A)$	해쉬함수에 A를 입력
$E_A(B)$	암호화키 A를 이용하여 B를 암호화
S_{AB}	A와 B사이의 고유 값

그림 2는 제안사항을 간단히 보여주는 예시이며 표 1은 그림 2에서 사용된 기호의 의미를 설명하고 있다.

4.성능분석

먼저 암호화를 하는데 드는 비용이 a, 복호화 하는데 드는 비용이 b, 그리고 초기 그룹키를 생성하고 분배하기 위한 비용이 c라고 할 경우 데이터 전송을 위한 비용(P)는 다음과 같이 나타낼 수 있다.

- 그룹키를 사용하지 않는 경우 : $P = (a+b)n$
- 그룹키를 사용하는 경우 : $P_G = a + c + bn$

위의 식에서 볼 수 있는 것처럼 $c < (n-1)a$ 인 경우 그룹키를 사용하는 것이 효율적인 것을 알 수 있다. 표 2는 제안된 메커니즘의 보안적인 특징을 보여준다.

표 2 제안사항의 특징

항목	평가
오버헤드	사용자 추가 시 그룹키를 전달해주는 오버헤드와 사용자간 고유값 측정을 위한 오버헤드 발생하지만 데이터 전달시 재 암호화 하는 과정이 없으므로 전체적으로 부하가 줄어듬
기밀성	그룹키는 사용자간 고유값으로 암호화 되며 데이터는 그룹키로 암호화되기 때문에 제 3자가 스니핑 기법으로는 알 수 없음
사회성	제안된 메커니즘의 그룹화를 통해 같은 관심사를 가진 사용자를 용이하게 연결하여 새로운 인맥 형성 및 데이터 공유가 가능

5.결론 및 향후계획

본 논문에서는 서버의 도움 없이 애드혹 네트워크 환경에서 같은 관심사를 가진 사용자간 그룹을 형성하고 안전한 소셜 네트워크 서비스를 위한 그룹키 형성 방법을 제안하였다. 그리고 그룹키를 사용하였을 경우와 그렇지 않은 경우에 대한 비교를 통해 그 효율성을 분석하였다. 향후에는 명성(reputation)을 기반으로 한 인증기법을 도입하여 데이터를 송수신에 따라 명성을 측정하고 해당 명성값을 기반으로 그룹에 가입을 승인하는 형태의 연구를 진행할 계획이다.

참고문헌

[1] Min Kyung Sung, Yon Dohn Chung, "소셜 네트워크 데이터의 프라이버시 보호 배포를 위한 모델", 정보과학회 논문지, 데이터베이스 제 37권 제4호, pp209-219, August 2010

[2] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication", Proceedings of the IEEE Int. Conf. on Comm., pp.4646-465, June, 2007

[3] Matthias Wilhelm, Ivan Martinovic, and Jens B. Schmitt. "On Key Agreement in Wireless Sensor Networks based on Radio Transmission Properties", Proceedings of the 5th Annual Workshop on Secure Network Protocols (NPSec), IEEE Computer Society, pp37-42, October 2009.