Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1353

상태 정보를 활용하여 악의적 사용자의 영향력을 최소화 하는 추천 알고리즘*

노 태 완,[1†] 오 하 영,[2‡] 노 기 섭,[3] 김 종 권[1]
[1]서울대학교, [2]숭실대학교, [3]대한민국 공군

State Information Based Recommendation Algorithm for Minimizing the Malicious User's Influence*

Taewan Noh,[1†] Hayoung Oh,[2‡] Giseop Noh,[3] Chong-Kwon Kim[1]
[1]Seoul National University, [2]Soongsil University, [3]Republic of Korea Air Force

요 약

최근 인터넷의 급성장과 함께 사용자들은 물건이나 영화, 음악 등을 구매 할 때 여러 가지 추천 사이트를 참고한다. 하지만 이러한 추천 사이트에는 악의적으로 아이템의 평점을 높이거나 낮추려는 악의적인 사용자 (Sybil)들이 존재하며, 결과적으로 추천시스템은 불완전하거나 부정확한 결과를 일반 사용자들에게 추천할 수 있다. 본 논문에서는 사용자 들이 생성하는 평점들을 안정상태 (stable state) 및 불안정상태 (unstable state)로 구분하고, 상태 정보를 활용하여 악의적 사용자의 영향력을 최소화 하는 추천 알고리즘을 제안한다. 제안하는 기법의 성능을 입증하기 위해 유명한 영화사이트에서 실제 데이터를 직접 수집 (crawling)하여 성능분석을 진행하였다. 성능분석결과 제안하는 기법의 성능이 기존 알고리즘 보다 향상됨을 확인하였다.

ABSTRACT

With the extreme development of Internet, recently most users refer the sites with the various Recommendation Systems (RSs) when they want to buy some stuff, movie and music. However, the possibilities of the Sybils with the malicious behaviors may exists in these RSs sites in which Sybils intentionally increase or decrease the rating values. The RSs cannot play an accurate role of the proper recommendations to the general normal users. In this paper, we divide the given rating values into the stable or unstable states and propose a system information based recommendation algorithm that minimizes the malicious user's influence. To evaluate the performance of the proposed scheme, we directly crawl the real trace data from the famous movie site and analyze the performance. After that, we showed proposed scheme performs well compared to existing algorithms.
Keywords: Recommendation system, Sybil, Social network

I. 서 론

최근 소셜 네트워크 서비스가 활성화되면서 사용자들에게 적합한 아이템들을 추천해 줄 수 있는 추천 시스템이 각광받고 있다. 이러한 추천시스템들은 사용자들에게 개인별로 차별화되고 정확한 아이템을 추천하기 위해서 여러 가지 추천 알고리즘을 사용하고 있다[1-6]. 또한 사용자들은 자신이 원하는 아이템

Received(07 .14. 2015), Modified(10. 22. 2015), Accepted(12. 03. 2015)
* 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구(No.NRF-2015R1A2A1A01007400) 및 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.NRF-2014R1A1A1003562)
† 주저자, twnoh@popeye.snu.ac.kr
‡ 교신저자, hyoh@ssu.ac.kr(Corresponding author)

에 대한 정보와 평점들을 보기 위해, 또는 자신에게 최적화된 추천을 받기 위해 추천시스템을 탑재 한 다양한 사이트들에게 직접 방문하여 서비스를 받고 있다. 해당 사이트들로는 왓차(watcha.net), 네이버 영화(movie.naver.com), 옥션(auction.co.kr) 등이 있다.

복잡한 인증이 필요한 기존 시스템과는 달리 추천 시스템들을 탑재한 서비스 사이트들은 다양한 사용자가 활용할 수 있게 하기 위해 특별한 보안 절차 없이 손쉽게 접근할 수 있는 구조이다. 결과, 악의적으로 자신이 원하는 영화나 아이템 등의 평점을 조작하는 시빌 공격(Sybil attack)이 일어날 수 있다. 시빌 공격이 발생했을 경우 해당 시스템은 거짓정보의 영향을 받아 정확한 추천을 수행하기 어려워진다. 실제로, 추천 사이트를 제공하는 영화 홍보 업체나 기업체에서 자신의 아이템이나 경쟁사의 아이템의 평점을 조작하는 일은 빈번하게 일어난다. 예를 들어 2014년 8월에 한 주류 업체는 경쟁자 업체가 자신의 제품에 고의적으로 악의적인 댓글을 단 이유로 검찰에 고소하는 일이 있었다[7]. 또한 영화 제작사에서 영화 홍보 업체에 돈을 주고 자신들의 영화에 호의적인 평점을 주도록 한 사실이 발각되어 사회적 이슈가 되었다[8]. 따라서 최근 이러한 시빌 공격을 방어할 수 있는 견고한 추천 시스템 (Robust Recommendation system)을 위한 방법들이 제시되고 있다. 하지만 기존 연구들은 추천 시스템의 초기 데이터 셋 (RS dataset)들이 시빌 공격의 영향을 받지 않은 정상데이터만으로 구성되어 있다고 가정하고, Random, Average, Bandwagon, Segment Attack 등과 같은 다양한 종류의 시빌 공격들을 임의로 생성하여 추천시스템의 견고한 수준을 향상시켰다[9-17].

공격 모델들에 대한 견고한 추천시스템 모델관련 기존 연구들은 다음과 같다. [18]에서는 타겟 아이템의 공격 전후의 통계적 특징을 이용하여 가까운 이웃 선택을 이용한 사용자 기반 추천 알고리즘을 제안했다. [19]에서는 정보 레벨 (Information level)을 이용하여 온라인 추천시스템의 시빌 공격을 방어해주는 기법을 제안했다. [20]에서는 악의적인 공격이 상대적으로 짧은 시간 안에 이뤄진다는 특징을 이용하여, 일정 시간 안에서의 아이템들의 평점 분포를 조사하여 시빌 공격을 탐지했다. [21]에서는 Dirichlet process과 latent factor들을 결합하여 평점을 예측하는 모델을 제안하고, 이 모델을 사용자의 클러스터링에 적용하여 시빌 공격을 탐지했다. [22]에서는 추천 시스템에서 분류된 (labeled) 데이터들과 분류되지 않은 (unlabeled) 데이터를 naïve Bayes classifier에 적용하여 다양한 시빌 공격을 탐지했다.

최근에는 목표 아이템에 대한 공격과 일반 유저처럼 보이기 위해 Filler item을 사용하는 Random attack과 Average attack의 성질을 이용하여 Robust RS를 제안한 논문도 있다[23]. [23]에서는 RDMA와 DegSim[24] 메트릭을 사용하여 일반 유저와 다른 시빌 유저들을 검출 한다. 이 논문의 알고리즘에서는 아이템이 시빌 공격을 받았다고 판별될 경우, 해당 아이템의 유저들을 모두 제거하게 된다. 하지만 만약 인기가 많은 아이템(selected item)을 이용하는 Bandwagon attack에 대해서는 이 알고리즘을 사용하지 못하는 큰 단점을 갖고 있다. 또한 [25]에서는 시빌 유저들간에는 긴밀한 상호연관성이 있다는 특징을 이용하여 그래프 방식의 알고리즘을 제안하였다. 실험 결과, 적은 수의 데이터에서는 높은 정확도를 보여준다. 그렇지만 데이터가 클 경우, 유저들간의 상호연관성이 떨어지는 단점이 발생하여 알고리즘의 성능이 떨어진다. 또한 두 개의 논문 모두 Movielens의 대해서만 실험을 진행하였기 때문에 다른 추천 사이트에서의 성능은 알 수가 없다.

시빌 공격은 크게 평점을 악의적으로 높이는 push attack과 평점을 악의적으로 낮추는 nuke attack으로 나뉠 수 있다. 시빌은 시빌 공격을 행하는 주체로 자신의 아이템의 평점을 높이기 위해서 정상적인 사용자들의 평점보다 아주 높은 점수를 주는 push attack을 수행하거나 경쟁사의 제품의 평점을 낮추기 위해서 낮은 점수를 주는 nuke attack을 수행할 수 있다. 하지만 시빌과 같은 악의적인 사용자는 아니지만 보통 다른 사람들과는 다르게 평점을 주는 사용자들도 존재할 수 있기 때문에 평균을 따르지 않는 정상적인 사용자들과 악의적인 사용자들을 구별하는 것은 어려운 문제이다.

본 논문에서는 초기 데이터는 정상적인 사용자들의 평점들로만 구성되어 있다고 가정하고 문제를 해결해왔던 기존 연구들과는 달리 현실성을 반영하여 연구를 진행한다. 즉, 기존의 데이터 셋들이 이미 악의적인 사용자나 평균을 따르지 않는 특이한 사용자들에 의해 이미 영향을 받았다고 가정하고, 이런 사용자들의 영향을 최소화하는 추천시스템을 제안한다.

II. 악의적 사용자의 영향력을 최소화하는 추천 알고리즘

제안하는 MMUI(Minimizing the Malicious User's Influence) 알고리즘은 사용자들이 아이템에 대해 평점을 줄 때, 해당 평점을 안정상태 (stable state) 혹은 불안정상태 (unstable state) 중 하나의 상태로 구분한다. 안정상태는 현재 평점을 매긴 사용자가 기존의 사용자들의 평균 평점들과 비슷하게 줬다는 것을 나타내고, 불안정상태는 분산 값이 매우 다르게 줬다는 것을 나타낸다. 즉, 불안정상태는 위에서 언급한 것과 같이 악의적인 사용자나 평균적 성향이 아닌 사용자들을 나타낸다. 제안하는 기법은 모든 평점들의 상태를 조사하여 평점이 불안정상태일 경우 해당 평점을 제거하여 추천 시스템의 정확도를 높여준다.

2.1 기호들

Fig.1은 본 논문에서 사용될 평점 매트릭스를 보여준다. 매트릭스는 아이템의 개수가 N개이고 각 아이템이 K개의 평점을 가질 수 있을 때 아이템에 대한 평점을 K x N의 평점 매트릭스 (rating matrix, RKxN)로 표현할 수 있다. ix는 x번째 아이템을 의미하며, x∈[1,N]이다. rx,1는 item x의 첫 번째 평점을 뜻하고, m(x)는 i_x의 평점의 개수이다.

Table.1은 본 논문에서 사용된 기호들을 설명한다.

	i_1	i_2	…	i_x	…	i_N
rating 1	$r_{1,1}$	$r_{2,1}$	…	$r_{x,1}$	…	$r_{N,1}$
rating 2	$r_{1,2}$	$r_{2,2}$	…	$r_{x,2}$	…	$r_{N,2}$
..	..	…	…	…	…	…
..	..	$r_{2,m(2)}$	…	…	…	…
..	..		…	$r_{x,m(x)}$	…	$r_{N,m(N)}$
rating K	$r_{1,m(1)}$		…		…	

Fig. 1. Matrix with the rating values, (R_{KxN})

Table 1. Notations

Notation	Description
N	The number of items
i_x	The xth item
$r_{m,n}$	Rating value for item n and user m
$i_{(x,mean)}$	Mean of item n
$i_{(x,STD)}$	Standard deviation of item n
m(x)	The total number of rating values of the item x
R_{MxN}	Rating matrix consist of user M and item N

2.2 초기 설정

평점의 안정 상태와 불안정 상태를 구별하기 위해서는 각 아이템들의 평균 (Avg.) 과 표준편차 (Standard deviation, STD)가 필요하다. 초기 설정에서는 이런 초기 값들을 설정해준다. 이 값들을 구하기 위해서 각 아이템들의 첫 번째 평점과 t개까지의 값을 이용하는데 이 논문에서는 t을 기본 값 (BASE COUNT)이라고 정의하였다.

초기 설정(Fig.2)에서는 1에서부터 N까지의 아이템들에 대해서 각 아이템의 첫 번째 평점의 값부터 BASE COUNT 번째의 평점의 값을 이용하여 각 아이템의 초기 평균과 초기 표준편차를 구한다.

Input: R_{KxN}, BASE COUNT
Output: $i_{(1,mean)}$, $i_{(2,mean)}$, … , $i_{(N,mean)}$
$i_{(1,STD)}$, $i_{(2,STD)}$, … , $i_{(N,STD)}$

1 for x=1 to N do
2 Calculate the average and STD of the item x from the first rating value to the BASE COUNTth rating values
3 end

Fig. 2. Initializations

2.3 평점의 상태 구별 알고리즘

평점의 상태 알고리즘은 각 아이템들의 평점들을 모두 조사하여 평점의 안정과 불안정한 상태를 구하

```
Input:  R_KxN, BASE COUNT
        i(1,mean), i(2,mean), ... , i(N,mean)
        i(1,STD), i(2,STD), ... , i(N,STD)
Output: R(MMUI)KxN

1  for x = 1 to N do
2  {
3    for y = 1 to m(x) do
4    {
5        z = (r_{x,y} - i_{(x,mean)}) / i_{(x,STD)}
6        if z < -1.0 or z > 1.0
7        {
8            Delete r_{x,y}
9        }
10       Calculate i_{(x,mean)}, i_{(x,STD)} by rating
         from 1 to rating y
11   }
12 }
```

Fig. 3. Algorithm for the analysis of the rating values per each item whether it is stable state or not

는 알고리즘이다.

악의적인 평점은 자신이 원하는 아이템의 평균 평점을 높이기 위해서 평점이 좋지 않은 목표 아이템에도 가장 높은 평점 값을 준다. 이러한 평점은 일반 사용자들의 평점 값에 비해 일반적이지 않은 성질을 갖게 된다. 만약 해당 평점의 정규분포가 -1.0미만, 1.0초과일 경우, 이 평점은 불안정한 상태의 평점으로 판단한다. 그리고 이 평점은 악의적인 유저가 매긴 평점으로 판단하고 삭제를 한다.

2.4 평점 예측

평점을 예측하기 위해서, 우리는 유저와 아이템의 성질을 숨겨진 요소들로 설명한 Matrix Factorization(MF) 방법을 사용하였다. 유저 m명과 아이템 n개 이루어진 평점 매트릭스를 R일 때 다음과 같이 나타낼 수 있다.

$$R \approx U^T V \tag{1}$$

$U \in R^{l \times m}$, $V \in R^{l \times n}$로써 각각 사용자와 아이템에 대한 행렬이고 l은 사용자와 아이템의 특성을 나타낸다. Singular Value Decomposition (SVD)방법을 이용하여 다음과 같이 줄인다.

$$\frac{1}{2}||R - U^T V||_F^2 \tag{2}$$

일반적으로 평점 매트릭스는 빈 부분이 대부분이므로 평점이 있는 부분만 이용하여 다음과 같이 나타낼 수 있다.

$$\min_{U,V} \frac{1}{2}\sum_{i=1}^{m}\sum_{j=1}^{n} I_{i,j}(R_{i,j} - U_i^T V_j)^2 + \lambda_1 \frac{1}{2}||U||_F^2 + \lambda_2 \frac{1}{2}||V||_F^2 \tag{3}$$

$I_{i,j}$는 유저 I가 아이템j에 대한 평점이 있는 경우에는 1, 없는 경우에는 0이 된다. 이 식을 기울기 하강(gradient descent) 방법을 통하여 행렬 R과 $U^T V$가 최소가 되는 지점을 찾는다.

III. 실 험

3.1 실험 설정

본 논문에서는 제안된 알고리즘의 성능 측정을 위하여 한국에서 가장 많이 사용하고 있는 네이버 영화 추천 사이트(http://movie.naver.com)를 활용하였다. 실험 데이터 확보를 위해서 2010년부터 2013년까지 개봉한 영화들에 대해서 직접 수집(crawling)을 수행하였다. 영화의 평점은 1~10점까지 줄 수 있으며, 한 사용자가 중복해서 같은 영화에 평점을 줄 수 는 없다. 또한, 각 영화마다 최대 평점개수는 10,000로 제한되어 있다. 2010~2013년에 개봉한 전체 영화 수 33,539 중에 101개 이상 평점이 존재하는 1,362개의 영화의 대해서만 진행하였다.

Table 2. Dataset information of the proposed scheme

Name	#items	#ratings	rating scale
Naver-movie	1,362	54,561	{1,2,...,10}

3.2 평점 개수에 따른 불안정한 상태비율

Fig.4는 평점수가 1000개에서 10000개까지인 영화들에 대해서 불안정한 상태부분의 비율을 백분율(%)로 표현한 것이다. 예를 들어 X축 1000은 평점수가 1000개에서 1999까지인 영화들, X축 9000은 평점수가 9000에서 10000까지의 영화들에 대한 결과이다. 그리고 이 실험에서는 BASE COUNT는 100으로 하였다. 먼저 평점 수가 많은 영화일수록 전체 상태들 중에서 불안정한 상태 부분이 낮아지는 것을 볼 수 있다. 영화의 평점 수가 많다는 것은 그 영화의 인기에 대응할 수 있다고 볼 수 있는데 많은 사람들이 평균에 근접하게 평점을 매기기 때문에 불안정한 상태 부분이 낮아지게 되고, 악의적인 사용자들의 부분이 작아지거나, 악의적 평점이 존재하더라도 전체 영향력이 감소하기 때문이다

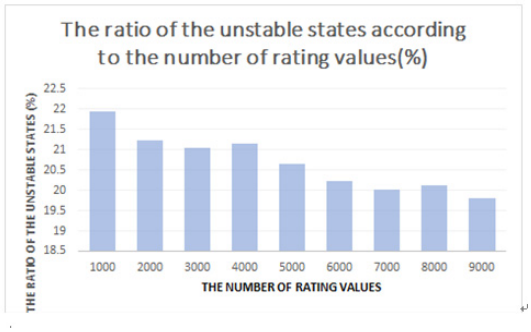

Fig. 4. The ratio of the unstable states according to the number of rating values

IV. 성능평가

4.1 실험 설정

Fig.5은 본 논문에서 사용한 실험 시나리오이다. MMUI알고리즘을 적용한 것과 아닌 것 두 가지 데이터 셋에 대해 80%의 Train set과 20% Test set으로 구성하였다. 80% Train set을 이용하여 20% 숨겨진 평점들을 예측하고 이 값들을 20% Test set과 비교하여 Mean Absolute Error (MAE)을 통하여 정확도를 분석하였다. 숨겨진 평점을 예측할 때 추천시스템에서 가장 많이 사용하고 있는 Matrix Factorization(MF)방식을 사용하였다. 또한 MMUI알고리즘과 비교하기 위해서 Least Trimmed Squares Matrix Factorization

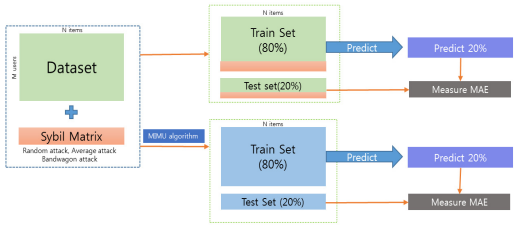

Fig. 5. Experiment Scenario

(LTSMF)방식을 사용하였다. LTSMF 방식은 MF 방식과 비슷하지만, 차이점은 가장 큰 잔차들의 제곱들을 사용하지 않음으로써, 특이점들로부터 멀리 떨어져 존재할 수 있도록 제안 된 방식이다. 각각 실험은 10번씩 진행하여 평균 값을 그래프로 나타내었다. MMUI의 BASE COUNT값은 100으로 설정하였다.

4.2 실험 결과

Fig.6은 직접 크롤링한 Naver-movie 데이터세트를 이용하여 MF, LTSMF[10] 그리고 MMUI의 MAE 비교를 비교한 것이다. MAE가 낮을수록 성능이 더 좋다는 것을 나타낸다. 기존 연구들은 이미 이전의 데이터들이 정상적인 사용자들의 평점들로만 구성되어 있다고 가정하고 임의의 시빌 유저들을 직접 만들어 대안들을 제시해왔다.

하지만 이미 기존의 추천사이트들은 악의적인 유저들로부터 영향을 받은 것이 현실이다. Naver-movie 데이터 역시 악의적인 유저로부터 이미 영향을 받았다고 생각될 수 있다. 오염된 이 데이터세트와 MF방식, LTSMF, 그리고 MMUI방식을 비교하였다.

Fig.6에서 보는 것과 같이 성능은 제안한 MMUI 알고리즘이 LTSMF와 단순히 MF 방식만

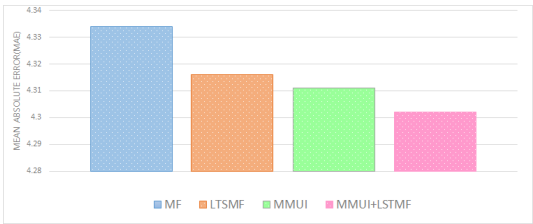

Fig. 6. The comparison of the performance between the proposed scheme and the previous work

사용한 것보다 높게 나온 것을 볼 수 있다. MMUI 방식은 평점을 예측할 때 MF방식을 사용하였다. 하지만 만약 MMUI의 MF방식 대신 LTSMF방식을 사용한다면 더 좋은 결과를 얻을 수 있다. 이 결과를 통해서 제안한 알고리즘이 불안정한 평점을 제거함으로써 다른 방법들과 비교해서 좋은 성능을 보인다.

V. Conclusion

현대 사회에서 규모가 큰 기업에서부터 작은 기업까지 자신의 제품들의 평점을 높이거나 상대방의 상품을 낮추기 위해서 악의적으로 평점사이트들의 아이템을 조작하는 경우가 빈번하다. 따라서 해당 사이트들의 데이터를 그대로 사용할 경우 제대로 된 추천을 할 없다. 본 논문에서는 기존의 시빌 공격에 대한 연구의 실험과는 다르게 최초로 데이터 셋이 이미 공격을 받았다고 가정하고 실험을 진행하였습니다.

References

〔1〕 Adomavicius, G., & Tuzhilin, A., "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions," Proceedings of the IEEE Transactions on Knowledge and Data Engineering, vol. 17, no. 6, pp. 734-749, June 2005

〔2〕 Ma, H., Zhou, D., Liu, C., Lyu, M. R., & King, I., "Recommender systems with social regularization," Proceedings of the fourth ACM international conference on Web search and data mining, pp. 287 - 296, Feb. 2014.

〔3〕 Lang, K., "News weeder: Learning to filter net news," Proceeding of the Twelfth International Conference on Machine learning, pp. 331 - 339. July 1995.

〔4〕 Linden, G., Smith, B., & York, J., "Amazon. com recommendations: Item-to-item collaborative filtering," Proceedings of the IEEE Internet Computing, vol. 7, no. 1, pp. 76 - 80, Feb. 2003.

〔5〕 Melville, P., & Sindhwani, V., "Recommender systems," Proceedings of the Encyclopedia of machine learning, pp. 829 - 838, 2010.

〔6〕 Melville, P., Mooney, R. J., & Nagarajan, R., "Content-boosted collaborative filtering for improved recommendations," Proceedings of the national conference on artificial intelligence, pp. 187 - 192, 2002.

〔7〕 News of the small businesses, http://news.kbiz.or.kr/news/articleView.html?idxno=36336

〔8〕 MBC news about the inaccurate RSs, http://imnews.imbc.com/replay/2013/nwdesk/article/3316638_11981.html

〔9〕 H. Yu, C. Shi, M. Kaminsky, P. Gibbsons and F.Xiao, "Dsybil: Optimal Sybil-Resistance for Recommendation Systems," Proceedings of the 30th IEEE Symposium on Security and Privacy, pp. 283-298, 2009.

〔10〕 Z. Cheng and N. Hurley, "Robust Collaborative Recommendation by Least Trimmed Squares Matrix Factorization," Proceedings of the 22nd IEEE International Conference on Tools with Artificial Intelligence, vol. 2, pp. 105-112, 2010.

〔11〕 Y. Koren, R. bell, and C. Volinsky, "Matrix factorization techniques for recommender systems," Proceedings of IEEE Computer, vol. 42, no. 8, pp. 30-37, Aug. 2009.

〔12〕 Mehta, B., Hofmann, T., & Fankhauser, P., "Lies and propaganda: Detecting spam users in collaborative filtering," Proceedings of the 12th international conference on intelligent user interfaces, pp. 14 - 21, Jan. 2007

〔13〕 B. Mobasher, R. Bruke, R. Bhaumik, and C. Williams, "Toward Trustworthy Recommender Systems: An Analysis of Attack Models and Algorithm Robustness," Journal of ACM Transcations on Internet Technology,

vol. 7 no. 4, Oct. 2007.
〔14〕 N. Hurley, "Robustness of Recommender Systems," Proceedings of the fifth ACM conference on Recommender systems, pp. 9-10, 2011.
〔15〕 Mehta, B., & Nejdl, W. "Attack resistant collaborative filtering," Proceedings of the 31st annual international ACM SIGIR conference on research and development in information retrieval, pp. 75 - 82, 2008.
〔16〕 J. Douceur, "The sybil attack," Proceedings of 1st International Workshop on Peer-to-Peer Systems, pp. 251-260, 2002.
〔17〕 B. Mobasher, R. Burke, and J. Sandvig, "Modelbased collaborative filtering as a defense against profile injection attacks," Proceedings of the 21st National Conference on Artificial Intelligence and the 18th Innovative Applications of artificial Intelligence Conference, vol. 2, pp. 1388-1393, 2006.
〔18〕 Gao Feng, "Robust Online Filter Recommended Algorithm based on Attack Profile," Proceedings of International Journal of Security and Its Applications, vol. 8, no. 4, pp. 253-264, July 2014.
〔19〕 Giseop Noh, Young-myoung Kang, Hayoung Oh, Chong-kwon Kim, "Robust Sybil attack defense with information level in online Recommender Systems," Proceedings of the Expert Systems with Applications vol. 41, no. 4, pp. 1781-1791, Mar. 2014.
〔20〕 Sheng Zhang, Amit Chakrabarti, James Ford, Fillia Makedon, "Attack Detection in Time Series for Recommendation Systems," Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 809-814, 2006.
〔21〕 Man Li, "Shilling Attack Detection Algorithm based on Non-random-missing Mechanism," Proceedings of the International Journal of Security and Its Applications, vol. 8, no. 6, pp. 115-126, 2013.
〔22〕 Jie Cao, Zhiang Wu, Bo Mao, Yanchun Zhang, "Shilling attack detection utilizing semi-supervised learning method for collaborative recommender system," Proceedings of the World Wide Web vol. 16, no. 5-6, pp. 729 - 748, Nov. 2013.
〔23〕 Wei Zhou, Junhao Wen, Yun Sing Koh, Shafiq Alam and Gillian Dobbie, "Attack detection in recommender systems based on target item analysis," Proceedings of the Neural Networks and International Joint Conference, pp. 332-339, 2014.
〔24〕 Zhuo Zhang, Sanjeev R. Kulkarni, "Detection of Shilling Attacks in Recommender Systems via Spectral Clustering," Proceedings of the Information Fusion and 17th International Conference, pp. 1-8, 2014.
〔25〕 P.-A. Chirita, W. Nejdl, and C. Zamfir, "Preventing shilling attacks in online recommender systems," Proceedings of the. 7th Annual ACM International Workshop on Web Information and Data Management, pp. 67-74, 2005.

〈저자소개〉

노 태 완 (Taewan Noh) 정회원
2013년 2월: 광운대학교 컴퓨터공학과 졸업
2015년 2월: 서울대학교 컴퓨터공학과 석사
〈관심분야〉 소셜 정보망, 추천시스템, 무선네트워크

오 하 영 (Hayoung Oh) 정회원
2002년 2월: 덕성여자대학교 컴퓨터공학과 졸업
2006년 2월: 이화여자대학교 컴퓨터공학과 석사
2013년 2월: 서울대학교 컴퓨터공학과 박사
2010년 4월~2010년 10월: U.C. Berkeley 방문연구원
2013년 3월~2013년 8월: 서울시립대학교 연구교수
2013년 9월~현재: 숭실대학교 정보통신전자공학부 조교수
〈관심분야〉 소셜 정보망, 추천시스템, 무선 네트워크 및 비디오 스트리밍

노 기 섭 (Giseop Noh) 정회원
1998년 2월: 공군사관학교 산업공학과
2009년 7월: 미국 콜로라도대학 전산학 석사
2014년 7월: 서울대학교 전기·컴퓨터공학과 박사
2014년 8월~현재: 대한민국 공군
〈관심분야〉 소셜 정보망, 추천시스템, 정보확산, DDoS, 스팸탐지 및 방어

김 종 권 (Chong-Kwon Kim) 정회원
1981년 2월: 서울대학교 산업공학과 졸업
1982년 2월: 미국 조지아공과대학교 산업공학과 석사
1987년 2월: 미국 일리노이대학교 전산학과 박사
1987년~1991년: 미국 Bellcore 통신 연구소 연구원
1991년~현재: 서울대학교 컴퓨터공학과 교수
〈관심분야〉 정보보호, 전자공학, 통신공학