Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.5, Oct. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.5.1235

안드로이드 앱 추천 시스템을 위한 Sybil공격과 Malware의 관계 분석*

오 하 영†‡
아주대학교

Relationship Analysis between Malware and Sybil for Android Apps Recommender System*

Hayoung Oh†‡
Ajou University

요 약

스마트 폰에서 활용할 수 있는 다양한 앱 (Apps)들의 개수가 기하급수적으로 증가함에 따라 개인 맞춤형 앱들을 추천해주는 시스템이 각광받고 있다. 하지만, 다양한 목적으로 악성 앱 (Malware)을 제작하여 구글 플레이 (GooglePlay) 사이트에 등록 후 배포하는 경우가 동시에 증가함에 따라 사용자들은 만족도 하강의 단순 피해부터 개인정보 노출 및 금전 탈취 등 심각한 수준의 많은 피해까지 겪고 있다. 또한, 소셜 네트워크가 발전함에 따라 물리적인 한 사용자가 많은 거짓 계정들을 만들어서 구글 플레이 사이트의 각 앱의 평점 (rating)들을 조작하는 시빌 공격 (Sybil)도 존재할 수 있다. 이때까지 악성 앱과 시빌 공격 연구는 독립적으로 진행되어 왔다. 하지만 실시간으로 발전하고 있는 지능화된 공격 종류들을 고려했을 때 악성 앱 제작자가 구글 플레이 사이트에 노출 된 평점까지 조작 후 인지도를 높여서 결국 악성 앱을 다운받도록 유도하는 지능화된 공격의 유무를 판단하는 것이 중요하다. 따라서, 본 논문에서는 구글 플레이어 사이트를 직접 크롤링하고 시빌 공격과 악성 앱의 상관관계를 실험적으로 밝힌다. 실험결과, 구글 플레이어 사이트에서는 아직 시빌과 악성 앱의 상관관계가 낮음을 알 수 있었다. 이는 악성 앱 배포자가 인지도 및 평점까지 다수 조작하여 많은 사람들에게 노출되면 다양한 Anti-Virus (AV) 벤더들에게 오히려 더 빨리 탐지되어 목적을 달성할 수 없기 때문에 이를 고려하지 않았거나, 악성 앱 배포자가 악성 앱을 만들고 배포하는 것에만 초점을 두고 사이트 인지도 및 평점 조작까지는 아직 동시에 고려하지 않음으로 해석될 수 있다.

ABSTRACT

Personalized App recommendation system is recently famous since the number of various apps that can be used in smart phones that increases exponentially. However, the site users using google play site with malwares have experienced severe damages of privacy exposure and extortion as well as a simple damage of satisfaction descent at the same time. In addition, Sybil attack (Sybil) manipulating the score (rating) of each app with falmay also present because of the social networks development. Up until now, the sybil detection studies and malicious apps studies have been conducted independently. But it is important to determine finally the existence of intelligent attack with Sybil and malware simultaneously when we consider the

Received(01. 05. 2016), Modified(1st: 05. 26. 2016, 2nd: 09. 06. 2016), Accepted(09. 07. 2016)
* "이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 한국연구재단에서 부여한 과제번호 : NRF-2014R1A1A1003562)"
† 주저자: hyoh@ajou.ac.kr
‡ 교신저자: hyoh@ajou.ac.kr(Corresponding author)

intelligent attack types in real-time. Therefore, in this paper we experimentally evaluate the relationship between malware and sybils based on real cralwed dataset of goodlplay. Through the extensive evaluations, the correlation between malware and sybils is low for malware providers to hide themselves from Anti-Virus (AV).

Keywords: Recommendation system, Sybil, Android App, Crawling, Correlation

I. 서 론

안드로이드 폰 및 아이폰 등 수많은 스마트 단말기들이 많이 애용됨에 따라 다운받고 활용할 수 있는 앱 (App)들이 기하급수적으로 증가되고 있다. 너무 많은 앱들은 사용자들이 개인별 맞춤형 앱을 선택하는데 혼란을 야기할 수 있고 특히 악성 앱이거나 만족도가 떨어지는 유료 앱을 다운받은 경우 사용자들에게 오히려 불편함을 줄 수 있다. 결과, 견고하고 개인 맞춤형 앱 추천 시스템이 필요하다. 기존의 악성 앱 연구는 앱 자체를 바이러스 토탈 (www.virustotal.com) 이라는 다양한 벤더 업체들이 서로 검증해주는 스캐너 기반의 악성 앱 탐지 방식과 악성 앱 제작 시 많이 사용되고 호출된 API함수간의 연관성 분석 및 유사도 비교 방식 등으로 나뉠 수 있다. 하지만 소셜 네트워크가 각광받게 됨에 따라 앱 제조자는 물론 다양한 사용자들이 앱에 대해서 의견 및 평점을 구글 플레이 사이트에 등록할 수 있다. 앱을 사용하기 전 사용자들은 보통 앱의 평점 및 리뷰들을 읽고 참고하기 때문에 정보가 왜곡되면 추천 시스템의 만족도가 떨어질 수 있다. 이와 관련 많은 연구들은 주로 영화, 책, 여행지 및 그 밖의 다른 아이템들의 데이터를 분석 후 견고한 개인맞춤형 추천 시스템 제공하기 위해 독립적으로 진행되었다. 즉, 이와 관련 많은 기존 연구들은 다양한 소셜 네트워크 사이트를 직접 크롤링 및 분석 후 아이템 별 평균평점과 큰 차이로 평점을 매기는 사용자 계정 (Sybil) [1] 및 공격받은 영화 (target item)들을 추적하거나 영향력을 최소화하는 기법들을 기반으로 견고한 추천 시스템을 제안했다 [2,3].

Fangzhao Wu 및 관련 저자들은 Twitter 및 Sina Weibo등과 같은 마이크로블로그 (micro blog)에서 문제 있는 계정 (sybil 혹은 spammer)와 시빌 행위에 따른 정보/메시지 왜곡(spam message)를 동시에 고려해서 두 가지 모두 탐지하는 방법을 처음으로 제안했다 [4]. 마이크로블로그란 한두 문장 정도의 짧은 메시지를 이용하여 여러 사람과 소통할 수 있는 블로그(blog)의 한 종류로, 웹상에서 지인과의 인간관계를 강화시키고 또 새로운 인간관계를 형성할 수 있도록 해주는 서비스인 일종의 '소셜 네트워크 서비스(Social Network Service, SNS)'이다. 기존의 다른 연구들이 시빌 탐지와 시빌 행위에 따른 정보 왜곡 탐지를 각각 독립적으로 분리해서 연구를 진행해온 것에 반에 Fangzhao Wu의 연구는 처음으로 스패머와 스팸 메시지를 동시에 고려한 통합적인 기법이기에 의미가 있다 [4]. 하지만, Fangzhao Wu가 제안하는 기법은 데이터 훈련 (training)과정 중에는 고려하지 않고 예측 (prediction)단계에서만 고려했고 마이크로블로그 작은 데이터 셋에서만 분석 및 검증해봤다는 한계점이 있다. 반면, 본 연구는 방대한 악성 앱 및 시빌 사용자의 스팸 정보(예: 평점, 댓글 등)를 직접 크롤링하고 악성 앱과 스팸 정보 간의 상관관계를 분석하기 위해 처음으로 이들을 동시에 고려해봤기 때문에 의미가 있다.

[5][6]에서는 앱 별 유사하게 사용된 API함수명 및 소스 코드에서 주로 호출되거나 사용된 단어들의 유사도를 비교 후 악성 앱을 탐지하는 방법을 제안했다. 하지만 아직까지 악성 앱을 구글 플레이에 올리는 제공자가 다수의 계정을 만들고 해당 앱에 대해 왜곡된 의견, 평점 및 다른 정상 사용자들의 댓글에 대한 댓글 등의 소셜 네트워크 정보를 동시에 고려한 연구는 없었다.

[14]의 저자는 좀 더 지능적인 공격자를 고려하기 위해서 시간에 따른 Sybil공격을 추적해서 동적으로 시스템을 방어하는 기법을 제안했다. 해당 시스템은 특정 시스템에 국한된 것이 아니기 때문에 아이템을 안드로이드 앱들로 가정한다면 악성앱 자체를 숨기기 위해서 동적으로 정보 노출을 변화시킬 수 있다. 하지만, [14]에서는 소셜 네트워크에서 각 노드사이에 존재하는 연결선(edge)의 변화를 동적으로 관찰하고 문제가 있는 Sybil을 방어하는 기법을 제안했기 때문에 해당 앱 혹은 아이템 등에 대해 왜곡된 의견, 평점 및 다른 정상 사용자들의 댓글에 대한 댓글 등의 상세한 소셜 네트워크 정보는 고려하지 않았다는 한계점이 존재한다.

반면, 본 논문에서는 소셜 네트워크 정보를 활용

하기 위해서 구글 플레이 사이트에서 관련된 정보들을 직접 크롤링 후 분석한 시빌 특성과 악성 앱의 연관성을 처음으로 분석했다. 악성 앱 탐지는 바이러스토탈로 검증했으며 시빌 공격은 비지도 학습 알고리즘을 통해 시빌 공격 유형 별 메트릭을 확률적으로 제안하고 직접 크롤링한 데이터에 접목하여 라벨링(labeling)했다.

II. 시스템 모델

2.1 가정 사항

기존 다양한 시스템에서 시빌의 원래 목적이 평점 조작을 바탕으로 인지도 혹은 매출을 높이는 단순한 목적 이였다면, 본 논문에서는 구글 플레이어 사이트에 올리는 악성 앱 제작자들은 악성 앱 등록은 물론 동시에 시빌 공격도 수행해서 인지도 및 평점을 조작하고 악성 앱이 인기있는 앱처럼 보이게 함으로써 사용자들의 앱 판매율을 늘일 수 있는 지능적인 공격자로 가정했다.

2.2 데이터 크롤링 및 전처리

제안하는 기법을 분석하기 위해 지난 2015년 10월부터 12월까지 구글 플레이어 게임 카테고리의 총 32개의 앱, 사용자 계정 총 146,842 및 평점을 크롤링했다. 모든 앱들 중 평균 평점 개수 이상으로 평점을 매긴 계정만 고려하기 위해서 식(1)을 만족하는 계정만 남기는 전 처리된 정보만 포함하도록 그림. 1과 같이 크롤링 매트릭스를 고려했다.

$$\text{Global rating of all apps}(G_i) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} \text{rating}_{ij} \quad (1)$$

식(1)에서 i는 i번째 사용자를, j는 j번째 앱을 의미한다. 결과, 그림.1과 같이 클롤링 한 데이터들 중에서 평균 개수 이상으로 평점을 매긴 사용자 계정들만 매트릭스에 유지한다.

2.3 다양한 시빌 공격 유형

일반적으로 추천 시스템에서 아이템은 크게 인지도 있는 인기 있는 아이템 (selected item), 타겟 아이템 (target item) 및 기타 채우는 아이템

	App 1	App 2	App 3		App N
User1	3		3		
User2	2	4	2		
User M-1		5	4		
User M		1	4		
# of rating users	2	3	4		
Global average # of users			3		
Average rating of each app i	2.5	3.3	3.25		
Global average rating of all apps					

Fig. 1. Matrix with the rating values, (RMxN)

(filler item)으로 구분된다. 정상 사용자와 시빌은 selected item, target item 그리고 filler item에 자유롭게 평점을 매길 수 있다. 만약 시빌이 target item에만 높은 평점을 매겨서 쉽게 인지도 및 매출을 올린다면 쉽게 탐지될 것이다. 따라서 시빌은 정상 사용자들과 최대한 유사해보이기 위해 selected item, target item 및 filler item에 아이템 별 평균을 고려해서 표 1과 같이 지능화된 형태로 나타난다.

특히, average공격은 공격자가 각 아이템 별 평균점수도 알 수 있다고 가정하고 filler items들에 대한 평점을 각각 아이템의 평균점수로 채워 최대한 정상 사용자 경향으로 나타나기 때문에 random공격에 비해서 더욱 탐지되기 어렵다는 특징이 있다.

Table.1 Various types of sybil attack

Attack type	Selected items	Filler items	Target item
Random	Not used	Normal Dist with Global mean	Max value
Average		Normal Dist with each item mean	
Bandwagon	Most rating items with max value	Normal Dist with Global mean	
Segment	Most popular items in a group	Min value	

III. 제안하는 기법

본 논문에서는 처음으로 견고한 안드로이드 앱을 추천하기 위해 악성 앱과 해당 앱에 대한 사용자들의 평균 평점 (average rating) 경향을 동시에 고려한다. 시빌은 다수의 계정을 만들어서 정상적인 사용자들처럼 보이면서 target item들의 평점을 높여 인지도 및 매출을 높이는 것을 목표로 하기 때문에 정상 사용자와 시빌을 구분해주는 메트릭 (metric)

을 제안한다. 특히, 시빌은 아니지만 평균 경향이 아닌 특이 사용자 (outlier)도 존재할 수 있기 때문에 사용자들을 크게 정상 (normal), 특이 사용자 (outlier) 및 시빌 공격 (Sybil)으로 나누고 각 사용자의 비율 및 악성 앱과의 관계를 분석한다. 마지막으로 virus total로 악성 앱이라고 판단된 앱들이 시빌과 어떤 관계가 있는 지 분석하고 원인을 규명한다.

3.1 시빌 탐지 메트릭

시빌 공격은 시빌 계정을 다수 만들고 최대한 정상 사용자처럼 보이기 위해서 표. 1과 같이 앱들을 세 가지로 분류하고 평점을 매긴다. 식 (2)는 시빌 공격 유형을 탐지할 수 있는 메트릭이고 표. 2는 본 논문에서 사용되는 기호들이다.

$$P_{sybil}(m) = \left(\alpha \cdot C_m^{\,O} + \beta \cdot C_m^{\,F} + \gamma \cdot C_m^{\,S}\right) \div T_{rating}(m) \quad (2)$$

$P_{sybil(m)}$는 사용자 m이 시빌 계정일 확률이다. 시빌은 target item들의 평점을 높이기 위해 랜덤으로 selected item 및 filler item들의 그룹을 선택하고 평점을 매긴다. 반면, 정상 사용자는 특별히 target item들을 고려하지 않고 자유롭게 인지도가 높은 selected item 및 기타 개인 성향에 따라 나머지 filler item들에 제 각각 평점을 매길 것이다. 따라서 사용자 m이 시빌 일수록 각 그룹 아이템인 target, selected 및 filler items들이 표.1과 같은 다양한 시빌 공격 경향을 따를 것이기 때문에 $P_{sybil(m)}$는 큰 값을 가질 것이다. 이를 위해 본 논문에서는 각 그룹 아이템에 가중치인 α, β, ɣ를 곱한 후 유저 m의 전체 평점 개수로 나눠서 사용자 m이 시빌 계정일 확률을 구한다.

각 가중치의 최적의 값은 현실적인 가정인 전체 사용자 계정 중 평균적으로 8%미만이 시빌 비율이라는 다른 연구들의 결과 [7][8], 크롤링 데이터의 특성 및 유형별 시빌 특성을 고려 후 충분한 실험을 통해 α= 0.10, β=0.35 및 ɣ=0.55로 결정됐으며 정상 사용자와 시빌의 구분 값인 $P_{sybil(m)}$는 0.3으로 검증했다.

Table. 2. Notations

$C_m^{\,O}$	The number of Outlier item with maximum rating value which user m rated
$C_m^{\,F}$	The number of Filler item which user m rated
$C_m^{\,S}$	The number of Selected item which user m rated
$P_{sybil}(m)$	Probability of user m being Sybil
$T_{rating}(m)$	The number of ratings by user m
R_{MxN}	Rating matrix consist of user M and item N

3.2 자기 조직화지도(Self Organizing Map:SOM) 기반 시빌 확률 분석

정상 사용자와 시빌의 구분 값을 통계적 방식으로 분석하여 검증하기 위해 비지도 학습의 데이터 마이닝 기법인 SOM을 이용 [11-13]하여 시빌 탐지 메트릭의 경계 값을 분석했다. 자기 조직화지도 알고리즘은 비슷한 속성들은 비지도 학습방식으로 클러스터링해서 자연스럽게 경계 값을 구해주는 지도(map)를 그려주기 때문에 정상과 시빌의 성격을 반영함으로써 궁극적으로 제안하는 기법에 사용될 수 있다. 즉, 정상과 시빌은 제안하는 메트릭 수식 (2)을 기반으로 서로 다른 특성을 보이기 때문에 맵에서 구할 수 있는 경계 값을 활용하면 시빌 탐지가 가능하며 또한 추후 맵의 각 클러스터링에 레이블(labeling)까지 가능하다면 다양한 종류의 시빌 종류들도 분석해 볼 수 있다.

Kohonen에 의해서 개발된 SOM기반 실시간 시빌 탐지 메커니즘은 크게 3단계로 이루어진다. 첫 번째는 전처리와 정규화 된 실험데이터로 탐지에 필요한 맵을 생성하는 학습 단계, 두 번째는 학습된 맵에서 정상 및 시빌 속성 상관관계를 활용한 각 클러스터 별 분류단계, 마지막으로 비지도 훈련 기반으로 실시간 탐지와 점진적 학습이 이루어지는 단계이다.

신경망 기법을 사용하는 클러스터링의 모델이면서 비지도 학습을 사용한다는 것이 특징인 SOM은 미리 정상과 시빌로 분류 (labeling)된 학습 데이터가 필요하지 않고, 분류되지 않은 학습 데이터를 넣어주

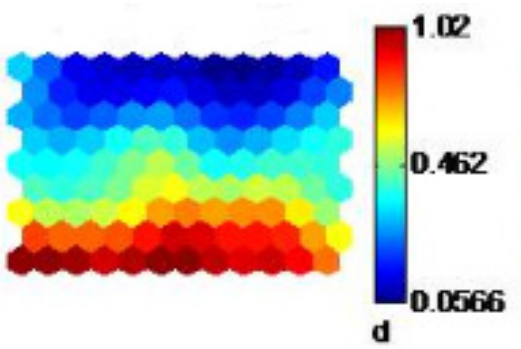

Fig. 2. Self Organizing Map (SOM)

면 비슷한 성격의 데이터끼리의 자아 클러스터링을 통해 알고리즘 스스로가 정상과 시빌 사용자 로 분류해준다. 또한 입력 데이터와 가장 가까운 뉴런의 이웃 뉴런들도 비슷한 방향으로 함께 학습시키기 때문에 인접한 뉴런들은 비슷한 성격을 가질 것이라고 예측 할 수 있다. 실험을 통해 정상과 시빌의 경계값이 그림. 2와 같이 0.3와 0.4사이의 값으로 수렴되는 것을 알 수 있다. 이는 앞서 언급한 실험기반의 휴리스틱 시스템 파라미터값이 의미가 있음을 보여준다.

3.3 시빌과 악성 앱 관계성 분석

소셜 네트워크가 활성화됨에 따라 일반 사용자들은 앱을 구매하기 전, 기존 다른 사용자들의 해당 앱에 대한 평점과 댓글을 반영한다. 본 논문에서는 다수 사용자 계정을 만들고 target item들에 최대값을 평점하는 시빌 계정들 중에 악성 앱 제작자들이 있을 수도 있다고 가정했다. 즉, 악성 앱 제작자는 구글플레이에 악성 앱을 올리고 해당 앱의 인지도를 높이기 위해서 시빌 계정으로 해당 앱들인 target items들에 최대값을 주는 지능화된 공격을 할 수 있다.

각 앱에 시빌 계정들의 비율이 얼마나 되는지 살펴보기 위해 아래와 같이 식 (3)를 정의했다.

$$\text{sybil ratio} = \frac{\sum_{i=1} \text{sybil}_{\text{IDi}}}{\sum_{i=1} \text{sybil}_{\text{IDi}} + \sum_{j=1} \text{normal}_{\text{IDj}}} \quad (3)$$

sybilIDi은 시빌확률 메트릭인 식(2)을 적용하여 0.3이상이 되는 시빌 계정을 의미하고, normalIDj은 0.3 미만인 정상계정을 의미한다. 결과, 악성 앱 종류 별 식(3)와 같은 시빌 비율 (sybil ratio)를 구하고 비례 관계가 있다면 상관관계가 높음을 알 수 있고 규칙성이 없다면 상관관계가 없음으로 판단할 수 있다.

IV. 성능평가

제안하는 기법의 성능을 검증하기 위해서 구글 플레이에서 표. 3과 같이 직접 크롤링했다. 또한, 앞서 언급했듯이 해당 데이터를 전처리 후 시빌확률 메트릭인 식(2)을 적용하여 0.3이상이 되는 사용자계정은 시빌 계정 sybilIDi으로, 0.3 미만인 사용자 계정은 정상계정 normalIDj으로 구분했다. 각 앱 별 시빌 비율을 살펴보기 위해 식(3)를 적용 후 실험결과는 그림. 3과 같다.

Table 3. Data Set

Name	#user	#Apps	category	Scale
google play	146,842	32	game	{1,2,,,5}

그림. 3을 통해 앱과 시빌은 특별한 연관성이 없음을 알 수 있다. 이는 아직까지 악성 앱 제작자가 소셜 네트워크 정보인 각 앱의 평균 평점 및 인기있는 앱등을 고려하지 않았거나 악성앱 제작자가 인위적으로 시빌 행위까지 동시에 하지는 않는 것을 알 수 있다. 이는 악성 앱 제작자가 시빌 행위를 할 경우 시스템 관리자가 평균 평점과 일정 값 (threshold Φ) 이상 큰 경우의 앱들은 target item들이라고 판단하고 일차적으로 견고한 앱 추천 시스템를 서비스 할 때 쉽게 악성 앱으로 탐지 될 수 있기 때문이다. 즉, 악성 앱 제작자의 궁극적인 의도는 실제 사용자들이 악성 앱을 다운받고 설치(installation)하는 순간 개인정보 및 금전탈취 등의 강한 공격을 목적으로 하기 때문에 평점 관리에 대해서는 최대한 정상적으로 보일 수도 있음을 알 수 있다.

본 논문에서 악성 앱 유무는 32개의 앱을 virus total에 테스트 하고 검증했다. 테스트 해본 결과, 2개는 악성앱 (Malware)로 나머지 30개는 정상앱 (Benign)으로 판별됐다. 즉, 앞서 언급했듯이 그림. 3을 통해 정상 앱들과 악성 앱들 사이에 시빌

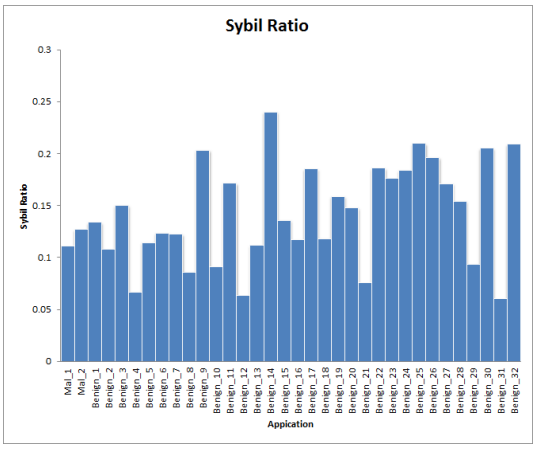

Fig. 3. Sybil ratio of each app

비율의 규칙성이 없음을 알 수 있다.

V. 결 론

안드로이드 앱에 대해서 많은 사람들이 다양한 의견 및 평점을 달수 있는 구글 플레이 (google-play) 사이트, 영화에 대해서 의견을 남기고 평점을 매길 수 있는 네이버 뮤비, 다움 무비, epinions, 일방적으로 팔로잉 (following)하고 관심사를 노출시킬 수 있는 마이크로블로그 Twitter, Sina Weibo등에 다양한 형태의 스팸공격이 나타나고 있다. 특히 스마트 폰 활용 등이 급격이 증가함에 따라 안드로이드 앱의 종류도 기하급수적으로 증가됐으며 그 중 다수의 앱들은 악성 앱 (Malware)이라는 것이 많은 벤더들에 의해서 밝혀졌다. 본 논문에서는 구글 플레이에서 직접 크롤롱한 데이터 분석 및 virus total을 통해 검증한 악성 앱을 활용해서 처음으로 시빌과 악성 앱의 관계를 분석했다. 다른 소셜 네트워크 사이트들과 달리 구글 플레이 사이트에서는 악성 앱 유포자가 인지도 조작 및 악성 앱 배포를 동시에 수행하는 악성 행위는 아직 하지 않는 것을 알 수 있다. 이는 아직까지 악성 앱 배포자가 소셜 네트워크까지 고려하는 지능적인 공격을 인지하지 못하고 있거나, 악성 앱 배포자가 오히려 인지도 및 평점까지 다수 조작하여 많은 사람들에게 노출되면 다양한 Anti-Virus (AV) 벤더들에게 더 빨리 탐지되어 목적을 달성할 수 없기 때문에 인위적으로 이를 동시에 고려하지 않는 것이다. 향후 연구로는 다양한 소셜 네트워크 데이터 셋[9]에서 시빌의 목적을 실험적으로 비교하고 샘플링의 사이즈[10]를 다양하게 고려해서 제안하는 기법을 정교하게 디자인하는 것이다.

References

[1] J. Douceur, "The Sybil attack," in Peer-to-Peer Systems, ser. Lecture notes in Computer Science. vol. 2429, pp. 251 - 260, 2002.

[2] 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, Jan. 2009.

[3] 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.

[4] Fangzhao Wu et al., "Social Spammer and Spam Message Co-Detection in Microblogging with Social Context Regularization", Proceedings of the 24th ACM International on Conference on Information and Knowledge Management, pp. 1601-1610, Oct. 2015.

[5] Arp D, et al., "Drebin: Effective and explainable detection of android malware in your pocket", Proceedings of the 21th Annual Network and Distributed System Security Symposium (NDSS '14), Feb. 2014.

[6] Kang H, Jang Jw, Mohaisen A, Kim HK, "Detecting and Classifying Android Malware using Static Analysis along with Creator Information", International Journal of Distributed Sensor Networks, vol. 11 no. 6, pp. 1-9, June. 2015.

[7] Jaehoon Lee et al., "Robust Recommender System considering additional short-answer evaluation on a Review Comments", Korea Institute of Information Security & Cryptology, Aug. 2015.

[8] Taewan Noh et al., "STA : Sybil Type-aware Robust Recommender System", KIISE Transactions on Computing Practices, Vol. 21, No. 10, pp. 670-679, Oct. 2015.

[9] Neil Zhenqiang Gong, Mario Frank, and Prateek Mittal, "SybilBelief: A Semi-Supervised Learning Approach for Structure-Based Sybil Detection", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9,

NO. 6, JUNE 2014.
〔10〕 Zhuo Zhang and Kulkarni, S.R., "Detection of shilling attacks in recommender systems via spectral clustering", Information Fusion (FUSION), 2014 17th International Conference on, Oct. 2014.
〔11〕 Hayoung Oh, Jiyoung Lim, Kijoon Chae and Jungchan Nah, "Home Gateway with Automated Real-Time Intrusion Detection for Secure Home Networks", Lecture Notes in Computer Science Volume 3983, pp 440-447, Jan. 2006.
〔12〕 Kyoungae Hwang, Hayoung Oh, Jiyoung Lim, Kijoon Chae and Jungchan Nah, "Traffic Attributes Correlation Mechanism based on Self-Organizing Maps for Real-Time Intrusion Detection", Information Processing Society Journal, Volume 12C, Issue 5, pp.649-658, Oct. 2005.
〔13〕 Hayoung Oh, "Unsupervised Scheme for Reverse Social Engineering Detection in Online Social Networks", KIPS Tr. Software and Data Eng, Vol. 4, No. 3, pp.129-134, April. 2015.
〔14〕 Changchang Liu et al., "Exploiting Temporal Dynamics in Sybil Defenses", ACM CCS, pp.805-816, Jan. 2015.

〈저자소개〉

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~2016년 8월: 숭실대학교 전자정보공학부 조교수
2016년 9월~현재: 아주대학교 다산학부대학 조교수
〈관심분야〉 소셜 정보망, 추천시스템, 무선 네트워크 및 비디오 스트리밍