Sosial şəbəkələrdə saxta profillərin aşkarlanması məsələləri

Yadigar İmamverdiyev[1] , Xəyalə Əhmədova[2]
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]yadigar@iit.science.az, [2]ehmedovaxeyale.97@mail.ru

***Xülasə*— Sosial şəbəkələr təkcə sosial ünsiyyət vasitəsi deyil, həm də real və virtual dünyada baş verən bədniyyətli hərəkətlərin inikas olunduğu kiberməkan, müxtəlif maraqların mübarizəsinin getdiyi meydandır. Adətən, bu bədniyyətli hərəkətləri həyata keçirən subyektlər öz kimliklərini saxta sosial şəbəkə profilləri vasitəsilə gizlətməyə çalışırlar. Bu saxta profillərin icra edəcəyi funksiyalar onları yaradanların niyyətinə görə dəyişir. Bu məqalədə sosial şəbəkələrdə saxta profillərin növlərinə, sosial şəbəkədən asılı olaraq yerinə yetirdiyi funksiyalara və törətdiyi fəsadlara baxılır, saxta profillərin aşkar edilməsi metodları analiz edilir.**

Açar sözlər — sosial şəbəkə; saxta profil; sosial bot; spam botu; saxta profillərin aşkar edilməsi,maşın təlimi.

I. GİRİŞ

Real aləmdə hər kəsin həyatda tutduğu mövqe ,məqsəd fərqli olduğu kimi, sosial şəbəkələrdə də insanların məqsədləri müxtəlif olur. Sosial şəbəkələr müxtəlif nöqtələrdə yaşayan insanların arasında müxtəlif məqsədlərlə qurulan virtual dünya kimi qarşılana bilər. Sosial şəbəkə anlayışı artıq çox insana aydındır. Sosial şəbəkələrdə yaradılan profillər hər zaman saf niyyətlərlə, yəni sadəcə həmin şəbəkənin yaxşı xüsusiyyətlərindən istifadə edilməsi məqsədilə yaradılmır. Məsələn, müzakirə forumlarında yaradılan saxta profil irqçiliyi və digər pis məqsədləri təbliğ edə bilər, bununla yanaşı sosial şəbəkələrdən nəticəsi zərərli olacaq çağırışlar etmək üçün də istifadə edilə bilir. Zərərli əməliyyatlar icra etmək üçün kimliyin saxtalaşdırılması saxta profillərin yaradılması sosial şəbəkələrin problemlərindəndir. Bu tip xoşagəlməz halların qarşısının alınması üçün saxta profillərin aşkarlanması üsulları işlənib, hazırlanmışdır.

II. ONLAYN SOSİAL ŞƏBƏKƏLƏRDƏ SAXTA PROFİLLƏR

Sosial şəbəkə anlayışı artıq uşaqdan-böyüyə hər kəsə aydındır. Sosial şəbəkələr müxtəlif məqsədlərlə yaradılır. Sosial şəbəkələrin funksionallığından tam yararlanmaq üçün çox vaxt bu sosial şəbəkələrdə profil açılması tələb edilir. Əgər bir şəxs özü haqqında (real) məlumatlarla bir profil yaratmış olarsa, o zaman bu profil real profil hesab edilir, çünki real bir şəxsə mənsub olmuş olur. Bununla yanaşı sosial şəbəkələrdə saxta profil anlayışı da vardır. Bu saxta profillərin məqsədi yaradıldığı sosial şəbəkədən asılı olaraq dəyişir. Sosial şəbəkələrə misal olaraq tanışlıq əsaslı sosial şəbəkələr, saf sosial şəbəkələr, müzakirə forumlu sosial şəbəkələr, işgüzar sosial şəbəkələr və s. göstərmək olar.

Tanışlıq əsaslı sosial şəbəkələrdə (Badoo, Match.com, BeautifulPeople və s.) saxta profilin məqsədi zəif görünümlü (emosional olaraq) insanı seçmək, onun bu zəif cəhətindən yararlanaraq bəzi məlumatları ələ keçirib, sonra təhdid yolu ilə pul tələb etmək ola bilər. Tanışlıq saytlarında bu tip əməllərlə məşğul olan insan “catfisher” adlanır [1, 2].

Ənənəvi sosial şəbəkələr (Facebook, Twitter, Orkut, Friendester və s.) saf niyyətlər üçün yaradılır, məsələn bir şəxs digəri tərəfindən bloklanıbsa, o zaman bloklanan şəxs saxta profil açıb yenidən onu bloklayan şəxsə dostluq təklifi göndərə, mesaj yaza və s. edə bilər.

Müzakirə forumlarında (Baidu Tieba, Quora, Skyrock və s.) saxta profillər irqçiliyi təbliğ edə bilər. Digərləri tərəfindən xoş qarşılanmayacaq mövzuları populyarlaşdıra bilər, yalan sorğular, məlumatlar paylaşa bilər ki bu halların da nəticəsi yaxşı bitməyə bilər [1].

İşgüzar sosial şəbəkələrdə (LinkedIn, Researchgate, Academia, Opportunity) saxta profillər bir başqasının gördüyü işləri özəlləşdirə bilər. Bu da qeyri-etikhərəkətdir [1, 3].

Media paylaşılan sosial şəbəkələrdə (Instagram, YouTube, Snapchat və s.) saxta profillər şəkil, video, mətn və s. paylaşmaq üçün istifadə edilir. Bəzən bir şəxs öz adı ilə etmək istəmir paylaşımları, məsələn, öz şəkillərini başqa ad altında paylaşır, bu yolla da artıq saxta profil yaratmış olur.

III. SAXTA PROFİLLƏRİN NÖVLƏRİ

A. Ələ keçirilmiş profillər (ing. Compromised profiles)

Bu tip saxta profillər real şəxslərə məxsus profillərdir. Profil sahiblərinin bu profil üzərində tam idarəsi olmur, yəni real sahiblər artıq bu profillər üzərində idarəni itirmiş

DOI: 10.25045/NCInfoSec.2018.13

olurlar. Bu da profilin bədniyyətlinin və ya hər hansısa bir zərərli proqramın əlinə keçməsinə gətirib çıxarır [4]. Buna səbəb profillərdə istifadə edilən sadə şifrələr ola bilər. Bu profillərin təhlükəli olmasının səbəbi real şəxsə mənsub olmasıdır, çünki bu real şəxs real aləmdə artıq nüfuza sahibdir. Bu da bədniyyətliyə real şəxs adından hərəkət etməyə kömək edir. Məsələn, bir şəxsin profili bədniyyətli tərəfindən ələ keçirilmişdirsə, bu zaman bədniyyətli real şəxs haqqında məlumatları şəxsin əlaqəsində olan insanlardan ala bilər.

B. Klonlanmış profillər (ing. Cloned Profiles)

Klonlanlanmış profillər saxta profillərin təhlükəli növlərindən biridir. Bu tip saxta profillərin ələ keçirilmiş profillərdən fərqi odur ki, klon hesab real şəxsə deyil, birbaşa bədniyyətliyə məxsus olur. Yəni ələ keçirilmədən birbaşa yaradılmış olur. Bu tip saxta profillərin 2 növü vardır:

- Saytdaxili profil klonlama (ing. Intra site profile cloning) – sosial şəbəkədə real, etibarlı profili olan şəxsin həmin şəbəkədə profilinin kopyasının (klonunun) yaradılması saytdaxili klonlama hesab edilir.
- Saytlararası profil klonlama (ing. İnter site profile cloning) – müəyyən bir sosial şəbəkədə profili olan şəxsin başqa bir sosial şəbəkədə bədniyyətli tərəfindən profilinin yaradılması saytlararası profil klonlama adlanır [5].

C. Kuklalar (ing. Sockpuppets)

Çorap kuklaları, əsasən, bir şəxsi və ya təşkilatı nüfuzdan salmaq və ya nüfuzunu artırmaq üçün istifadə edilən obrazlardır. Əgər hər hansı xəbər bülletenində (ing. news blog), sosial şəbəkədə və ya hər hansı müzakirə forumunda eyni şəxsə aid olan 2 müxtəlif hesab mövcuddursa, o, sockpupet cütü (ing. suckpuppet pair) adlanır [6]. Bu hal nüfuzlu bir şirkətə rəqib olan təşkilatın kuklalardan istifadə edərək hədəf təşkilatın nüfuzuna xələl gətirəcək paylaşımlar etdiyi və ya yorumlar bildirdiyi zaman baş verir. Çorap kuklaları reklam sahəsində istifadə edilərək təşkilatın, məhsulun və ya şəxsin nüfuzunu artırmaq üçün istifadə edilə bilər.

D. Sibil hesablar (ing. Sybil Accounts)

Bir şəxsin çox sayda yaratdığı və əl ilə idarə etdiyi saxta hesablar sibil hesablar adlanır. Bu hesablar sosial şəbəkələrdə spam, zərərli proqram yaymaq və qeyri-mütənasib böyüklükdə təsir əldə etmək üçün istifadə edilir. Sibil hücumçuların pis rəy vermək, qeyri-qanuni səs vermək, resurslara giriş əldə etmək, təhlükəsizlik və gizliliyi pozmaq və s. kimi məqsədləri olur [7].

E. Botlar saxta profil kimi (ing. Bots as Fake Profiles)

İş baxımından botlar sibil hesablara oxşardırlar, amma əsas fərq botların avtomatlaşdırılmış kompüter proqramları olmasıdır. [8]-də müəlliflər funksionallığına əsaslanaraq botları 5 kateqoriyaya ayırırlar:

- ***Spam botları*** – Spam botları, xüsusilə, şəxsi bloqlara keçid, ödəmə məzmunlu, reklam məzmunlu və s. tipli zərərli məzmunları şəbəkədə istənməyən çox sayda əlaqələr qurmaqla yaymaq üçün yaradılan kompüter proqramıdır [9].
- ***Sosial botlar*** – Sosial botlar maksimum sayda istifadəçiyə çatmaq və yoluxdurmaq üçün özlərini virus kimi ictimaiyyətə tanıdan proqramlardır. Daha bir tədqiqat [9] bu botlara onlayn sosial şəbəkələrdə hesabları idarə edən və real istifadəçilərin hərəkətlərini təqlid edən botlar kimi yanaşır. Sosial botlar hər zaman problem yaratmırlar. Onlar da işlərinə görə digər botlar kimidirlər, amma onların əsas diqqət mərkəzi daha çox onlayn insanlarla sosial əlaqələr qurmaqdır.
- ***Bəyənmə botları*** (ing. Like bots) – paylaşımlara, rəylərə gələn bəyənmə sayının saxta yolla artırılması üçün istifadə edilir. Reklamda bəyənmə botları məhsula olan inamı artırmaq üçün istifadə edilə bilər [5].
- ***Təsir botları*** (ing. İnfluential bots) – şəbəkə təsir botları Facebook və Twitter kimi onlayn sosial şəbəkələrdə qanunsuz olaraq hər hansı mövzunu məşhurlaşdırmaq, fikirlərə təsir etmək üçün istifadə edilən avtomatlaşdırılmış kimliklərdir [10]. Şəbəkədə təsir botlarının əsas işi onlayn sosial şəbəkələrdə xüsusi mövzu və ya məhsul haqqında istifadəçilərin fikirlərini dəyişməkdir.
- ***Botnet*** – Onlayn sosial şəbəkələrdə avtomatlaşdırılmış kompüter proqramlarının şəbəkəsi Botnet adlanır.Bu şəbəkədəki hər bir bot fərqli və ya oxşar əməliyyatlar icra etmək üçün təyin edilir. Botnet idarə kanalı (ing. control-channel) vasitəsilə qanunsuz fəaliyyətlər göstərmək üçün idarə edilən kompüter proqramları toplusudur [11].Botnetlər, adətən, “botmasters” adlanan istifadəçilər tərəfindən zərərli məqsədlər üçün idarə edilir.

IV. SOSİAL ŞƏBƏKƏLƏRDƏ SAXTA PROFİLLƏRİN AŞKARLANMASI METODLARI

Müəlliflər [12]-də Twitter və Facebook-da ələ keçirilmiş hesabları aşkarlamaq üçün COMPA adlanan alət təklif edirlər. Müəlliflər göndərilən mesajların əlamətləri əsasında statistik modelləşdirmə vasitəsilə istifadəçilərin davranış profillərini yaradır və anomaliya hesabını hesablamaq üçün n-qram analizi kimi bir neçə oxşarlıq metrikasından istifadə edirlər. Əlamətlərin çəkiləri SMO (Sequential Minimal Optimization) metodu ilə müəyyən edilir. [13]-də müəlliflər Facebook-da spam kompaniyalarını divar mesajlarının klasterləşdirilməsi əsasında təyin edirlər. Sonra hər bir zərərli

hesabın ələ keçirilmiş hesab olması divarda çıxan kontent (şəkillər, videolar və s.) əsasında analiz edilir.

Klonlanmış hesabların aşkarlanması üçün də bir sıra tədqiqatlar vardır. [14]-də müəlliflər Markov Clustering (MCL) alqoritmindən istifadə edərək Facebook şəbəkəsini oxşar cəhətlərə əsaslanaraq daha kiçik klasterlərə bölüblər və real profillərə oxşar bütün profillərin klon olub-olmadığının müəyyən edilməsi məqsədilə əlaqə gücünün hesablanması üçün toplanıblar. Digər bir tədqiqatda [15] müəlliflər sosial şəbəkədə saxta profillərin aşkarlanması üçün 3 komponentdən ibarət olan sistemin modelini təklif edirlər. “Informasiya distilyatoru” (ing. information distiller) adlanan birinci komponent real istifadəçilərdən informasiya çıxarıb, şəxsi yeganə şəkildə müəyyən etmək üçün istifadə edilə biləcək əlamətləri seçir. “Profil ovçusu” (ing. profile hunter) informasiyanı işləyir və istifadəçilərin profillərini müxtəlif sosial şəbəkələrdə tapır. “Profil verifikatoru” (ing. profile verifier) bütün profillər arasında oxşarlıq hesabını hesablayır və nəticəni istifadəçiyə təqdim edir.

Sosial şəbəkələrdə kukla hesablarını müəyyənləşdirmək üçün də bir sıra tədqiqatlar aparılmışdır. [16]-dakı tədqiqatda Tianya forumu və Taobao onlayn auksion saytında maraq doğuran mövzular əsasında istifadəçilərin şəbəkəsi (qrafı) yaradılmışdır. İstifadəçilərin yazı stillərinə əsaslanaraq, müəllif kukla şəbəkəsini əldə etmək üçün qrafı emal etmiş və bu qrafda kukla topluluqlarını aşkarlamaq üçün icma aşkarlama metodlarını tətbiq etmişdir. Hong Kong əsaslı müzakirə forumunda olan kuklaları aşkarlamaq üçün başqa bir metod [6]-da təqdim edilib. Bu metod bir hesab tərəfindən paylaşılan mövzuların və digər hesablar tərəfindən verilən cavabların ümumi sayına əsaslanır. Kukla cütünü tapmaq üçün aşkarlama qiyməti hesablanır. Qiymət nə qədər böyükdürsə, iki hesabın kukla cütü olması şansı da bir o qədər artır. İstifadəçilərin durğu işarələri sayı, sitat gətirmək sayı, böyük və ya kiçik hərflərin istifadəsi kimi əlamətlərinə əsaslanaraq [17]-dəki müəlliflər Wikipedia şəbəkəsi üçün təbii dilin emalı metodlarından istifadə edərək kuklaların aşkarlanması metodunu təqdim edirlər.

Tədqiqatçılar sosial şəbəkələrdə [7, 18, 19, 20] sibil hesabların aşkarlanmasına da diqqət yetirirlər, lakin sibil hücumların aşkarlanması hələ ilkin mərhələdədir. Sibil müdafiə metodlarının əksəriyyəti bir hesabın real hesaba nə dərəcədə yaxşı əlaqəli olmasına əsaslanaraq hesabların ranqlaşdırılması metodu ilə işləyir. Əgər hesab real hesablar toplusu daxilindədirsə, onun ranqı daha böyük olur. SybilGuard-da [21] müəlliflər sosial şəbəkəni Sibil hücumlardan qorumaq üçün yeni bir yanaşma təqdim edirlər. Onlar iki hesab arasındakı əlaqəni inam əlaqəsi kimi qəbul edirlər. Sibil hesablar etibarlı hesablardan etibarlı əlaqə istifadə edilməklə fərqləndirilir. SybilGuard, əsasən, sosial şəbəkələrin iki xüsusiyyətindən asılıdır: birincisi etibarlı hesabların hər zaman çox sayda əlaqəsi olur, ikincisi saxta istifadəçilər az etibarlı əlaqələri olan çox sayda hesablar yaradırlar. [22]-də müəlliflər Facebook heyran (ing. fan) səhifələri, əlaqələr, aktiv dostlar və s. kimi əlamətlərdən istifadə edərək saxta profilləri təyin etmək üçün Facebook şəbəkəsinin real verilənlərinə MCL alqoritmini tətbiq edirlər. MCL istifadəçiləri 3 klasterə ayırır, onlardan biri bütün saxta kimlikləri, ikincisi bütün normal profilləri və üçüncüsü bu ikisinin qarışığını ehtiva edir. Bu tədqiqat göstərdi ki, decision tree (DT), Support Vector Machine (SVM), Naïve Bayes (NB) və s. kimi metodlar profilləri saxta və ya real siniflərə ayırmaq üçün bir vasitə ola bilər, ancaq çox sayda sinfə sahib sosial şəbəkə profili verilənlər toplusu üçün səmərəli işləmir. Həmçinin, bu cür yaxşı müəyyən edilmiş profil verilənləri toplularının çatışmazlığı var və verilənlərin əksəriyyəti əvvəlcədən təyin edilmiş sinif nişanı və ya əlamətləri müəyyənləşdirmir, buna görə də, təlimsiz metodlar təlimli metodlardan üstündür. Eynilə, Bayes klassifikatoru və k-means klasterləşdirmə tətbiq etməklə cins və yer əlamətlərini istifadə edərək Twitter-də aldatmanın aşkarlanması üçün [23]-dəki müəlliflər tərəfindən yeni bir yanaşma təklif edilmişdir. [24]-də müəlliflər bal profilləri (ing. honey profiles) ilə əlaqəli olan istifadəçilər arasından spammerləri təyin etmək üçün Random Forest (RF) alqoritminə əsaslanan klassifikator təklif edirlər. Spam strategiyasına əsaslanaraq spam profillərinin Displayer, Bragger, Poster və Whisperer adlanan 4 kateqoriyası fərqləndirilir.

Spam botlarının aşkarlanması da bir neçə tədqiqatçı tərəfindən araşdırılır. [25]-dəki müəlliflər göstərir ki, 4 klassifikasiya metodundan (DT, SVM, K-nearest neighbor və neyron şəbəkələri) başqa, Bayes klassifikatoru Twitter şəbəkəsində spam botlarının ən yaxşı aşkarlama metodudur. [10]-dəki tədqiqatın müəllifləri sosial şəbəkədə təsirli botları aşkar etmək üçün üç addımdan ibarət olan bir yanaşma təklif edirlər. İlk addımda botlar əllə yoxlama, davranış analizi və linqvistik bilik kimi ilkin metodlarla təyin edilir. İkinci mərhələdə əksər botlar klasterləşdirmə, kənarlaşma (ing. outliers) və şəbəkə analizi əsasında müəyyən edilir. Üçüncü addımda isə qalan botlar test məlumatları kimi əvvəlki addımlarda müəyyən edilmiş botlar və insanlardan istifadə etməklə təyin edilirlər.

Saxta profillərin aşkarlanması tədqiqatlarında ən çox SVM, DT və Bayes klassifikasiya alqoritmləri istifadə edilir. Bundan əlavə, tədqiqatçıların əksəriyyəti tədqiqat aparmaq üçün Twitter sosial şəbəkəsindən istifadə edirlər. Bunun səbəbi Twitter-in tədqiqat məqsədli istifadəçi verilənlərinə girişə icazə verməsi ola bilər.

Sosial şəbəkələrdə saxta hesabların aşkarlanması üçün maşın təliminə əsaslanan müxtəlif metodlar tətbiq edilir, lakin tədqiqatçıların fikirlərini sadəcə xüsusi tip saxta profillərə cəmləməsi digər tip saxta profillərin aşkarlanmamasına və bədniyyətlilərin şəbəkəni çirkləndirməsinə gətirib çıxarır. Buna görə də, sosial şəbəkələrdə maksimum sayda saxta profilləri aşkarlaya bilən ümumi metodların işlənməsi çox aktualdır. Bundan əlavə, zaman keçdikcə sosial şəbəkələrdə istifadəçilər və onlar tərəfindən yaradılan məzmunun sayı sürətlə artır və saxta hesabları aşkarlamaq daha da çətinləşir. Buna görə, anomal davranışı müəyyənləşdirmək və ya sosial şəbəkələrdə analiz aparmaq üçün böyük ölçülü qrafların analizi, qrafın

bölünməsi və klasterləşdirilməsi alqoritmləri üçün yaxşı miqyaslanan maşın təlimi metodlarına böyük ehtiyac vardır [5].

NƏTİCƏ

Sosial şəbəkələr kənardan necə rəngarəng görünsə də,istifadəçinin məqsədinə görə təhlükəli alətə də çevrilə bilir.Bu tezisdə saxta profillərin növündən və yaradıldığı şəbəkədən asılı olaraq yerinə yetirdiyi funksiyalardan bəhs edildi.Saxta profillərin aşkarlanması metodları və bu barədə kiber qanunlar saxta profillərin istifadəsi zamanı meydana çıxan xoşagəlməz halların qarşısının alınması,bu halların azaldılması üçün işlənib hazırlanmışdır.Maşın təliminə əsaslanan metodlardan əlavə hər bir şəxs sosial şəbəkədə təhlükəsizliyini təmin etmək üçün sadə parollardan istifadə etməməlidir və parollarını mümkün qədər gizli saxlamalıdır.

ƏDƏBİYYAT

[1] M.A. Wani, M.A. Sofi, S.Y.Wani,” Why fake profiles: A study of anomalous users in differentcategories of Online Social Networks”, International Journal of Engineering Technology Science and Research , vol. 4, pp. 2394 – 3386, September 2017.

[2] Making Technology easier, bobology- What is a Catfisher? https://www.bobology.com/public/What-is-a-Catfisher.cfm.

[3] CS Blog, A computer scientist’s research blog. http://ptbcs.blogspot.com/2015/09/rg-fails.html.

[4] D. Savage, X. Zhang, X. Yu, P.Chou, and Q.Wang, “Anomaly detection in online social networks”, Social Networks, vol.. 39, pp.62-70, 2014.

[5] M.A.Wani , S. Jabin , G. Yazdani , N. Ahmad, “Sneak into devil’s colony – A study of fake profiles in Online Social Networks and the cyber law” arXiv preprint arXiv:1803.08810, 2018.

[6] X. Zheng, Y.M. Lai, K.P. Chow, L.C. Hui, S.M. Yiu, “Sockpuppet detection in online discussion forums”, Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011, pp. 374-377. IEEE, October 2011.

[7] P. Gao, N.Z. Gong, S.Kulkarni, K.Thomas, and P.Mittal, “Sybilframe: A defense-in-depth framework for structure-based sybil detection”, arXiv preprint arXiv:1503.02985, 2015.

[8] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, “The rise of social bots”, arXiv preprint arXiv:1407.5225, 2014.

[9] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, “Design and analysis of a social botnet”, Computer Networks, vol. 57(2), pp. 556-578, 2013.

[10] V.S. Subrahmanian, A. Azaria, S. Durst, V. Kagan, et al, “The DARPA Twitter bot challenge”, arXiv preprint arXiv:1601.05140, 2016.

[11] S.S. Silva, R.M. Silva, R.C. Pinto, and R.M. Salles, “Botnets: A survey”, Computer Networks, vol. 57(2), pp. 378-403, 2013.

[12] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, “COMPA: Detecting Compromised Accounts on Social Networks”, NDSS, February 2013.

[13] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, “Detecting and characterizing social spam campaigns”, Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, pp. 35-47.ACM, November 2010.

[14] M. Y. Kharaji, and F. S. Rizi, “An IAC Approach for detecting profile cloning in Online Social Networks”, arXiv preprint arXiv:1403.2006, 2014.

[15] G. Kontaxis, I. Polakis, S. Ioannidis, and E. P. Markatos, “Detecting social network profile cloning”, IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 295-300, March 2011.

[16] Z. Bu, Z. Xia, and J. Wang, “A sock puppet detection algorithm on virtual spaces”, Knowledge-Based Systems, vol. 37, pp. 366-377, 2013.

[17] T. Solorio, R. Hasan, and M. Mizan, “A case study of sockpuppet detection in wikipedia”, Workshop on Language Analysis in Social Media (LASM) at NAACL HLT, pp. 59-68, June 2013.

[18] J. R. Douceur, “The sybil attack.”, Peer-to-peer Systems, pp. 251-260, Springer Berlin Heidelberg, 2002.

[19] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai, “Uncovering social network sybils in the wild”, ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 8(1), pp. 5-33, 2014.

[20] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, “Sybillimit: A near-optimal social network defense against sybil attacks”, IEEE Symposium on Security and Privacy, pp. 3-17, May 2008.

[21] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman “Sybilguard: defending against sybil attacks via social networks”, IEEE/ACM Transactions on Networking, , vol. 16(3), pp. 576-589, 2008.

[22] K. Lee, J. Caverlee, and S. Webb, “Uncovering social spammers: social honeypots+ machine learning”, Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval, pp. 435-442, ACM, July 2010.

[23] J. S. Alowibdi, U. A. Buy, S. Y. Philip, S. Ghani, and M. Mokbel, “Deception detection in Twitter”, Social Network Analysis and Mining, vol. 5(1), pp. 1-16, 2015.

[24] G. Stringhini, C. Kruegel, and G. Vigna, “Detecting spammers on social networks”, Proceedings of the 26th Annual Computer Security Applications Conference, pp. 1-9, ACM, December 2010.

[25] A. H. Wang, “Detecting spam bots in online social networking sites: a machine learning approach”, IFIP Annual Conference on Data and Applications Security and Privacy XXIV, pp. 335-342, Springer Berlin Heidelberg, 2010.

ISSUES OF DETECTION FAKE PROFILES IN SOCIAL NETWORKS

Yadigar İmamverdiyev, Khayala Ahmedova

[1,2]Institute of Information Technology of ANAS,

Baku, Azerbaijan

[1]yadigar@iit.science.az, [2]ehmedovaxeyale.97@mail.ru

Abstract – Social networks are not only a means of social communication but also they are the cyber area where malicious acts occurring in the real and virtual world are reflected and the square in which different interests struggle. Normally, those who commit these bad actions try to hide their identity through fake social networks profiles. The functions of these fake profiles differ from one another depending on the purposes of those who create them. This article involves looking at the types of fake profiles, the functions they perform depending on the social network, the complications they have created, and the methods used to detect fake profiles have been analyzed.

Keywords – the social network, fake profile, social bot, spambot, detection of fake profiles, machine training.