PARADIGMA, No.1, 2025, səh.136-141
https://doi.org/10.30546/30015.2025.1.057

KİBERTƏHLÜKƏSİZLİKDƏ SOSİAL ŞƏBƏKƏ ANALİZİ: RİSKLƏRİN VƏ TƏHLÜKƏLƏRİN AŞKARLANMASI

N.Ə. Həsənova, E.A. Səmədzadə
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: Elshan.Samadzada@student.au.edu.az

Xülasə. Sosial Şəbəkə Analizi (SNA), şəbəkə daxilindəki əlaqələrin təhlilinə əsaslanan yanaşma kimi kibertəhlükəsizlik sahəsində mühüm vasitəyə çevrilmişdir. Məqalədə kibertəhlükələrin aşkarlanması məqsədilə aralıq, dərəcə, yaxınlıq mərkəzliyi kimi qraf metrikləri və icma aşkarlanması üsulları tədqiq olunur. Araşdırmanın əsas məqsədi sosial şəbəkə strukturlarını təhlil etməklə kibertəhlükələrin müəyyənləşdirilməsi və qarşısının alınması imkanlarının qiymətləndirilməsidir.

Açar sözlər: Sosial şəbəkə analizi, kibertəhlükəsizlik, kibertəhdidlər, qraf metrikləri, qraf nəzəriyyəsi, sosial platformalar.

Giriş

Bugünkü rəqəmsal dövrün ən əhəmiyyətli inkişaflarından biri, sosial şəbəkələrin həyatımıza güclü təsir etməsi və bununla paralel olaraq kibertəhlükəsizlik sahəsində yeni çağırışların meydana gəlməsidir. Sosial şəbəkələr, məlumat mübadiləsi, insan əlaqələri və şəxsiyyətlərin bir-biri ilə qarşılıqlı təsiri baxımından böyük bir rol oynayır. Lakin, bu platformaların təklif etdiyi əlaqə imkanları, eyni zamanda istifadəçilər üçün təhlükəsizlik riskləri yaratmaqda, daha geniş mənada isə cəmiyyət üçün potensial təhlükələrə səbəb olmaqda davam edir. Bu vəziyyətdə, **Sosial Şəbəkə Analizi (Social Network Analysis - SNA)**, şəbəkələrdəki əlaqələri, strukturları və qarşılıqlı təsirləri izləyən bir yanaşma olaraq kibertəhlükəsizlik sahəsindəki ən mühüm alətlərdən birinə çevrilmişdir. Sosial şəbəkə analizinin tətbiqi, yalnız fərdi məlumatları qorumaqla qalmır, həm də şəbəkələrdəki potensial təhdidlərin aşkar edilməsini təmin edir. Bu metod, həmçinin təhdidlərin öncədən proqnozlaşdırılmasına və risklərin minimuma endirilməsinə kömək edir. Eyni zamanda, sosial şəbəkə analizinin kibertəhlükəsizlikdəki tətbiqləri, zərərli fəaliyyətlərin və sosial mühəndislik hücumlarının daha sürətli şəkildə tanınmasına və qarşısının alınmasına şərait yaradır. Bu metodun gücü, şəbəkələrdəki əlaqələrin izlənməsi və riskli davranışların müəyyənləşdirilməsindəki incəliklərdə yatır. Təhlükəsizlik sahəsindəki mütəxəssislər, sosial şəbəkə analizini yalnız hücumların təhlili üçün deyil, həm də etibarlı məlumat axını və təhlükəsizlik infrastrukturu yaratmaq üçün vacib bir vasitə olaraq görürlər.

Sosial şəbəkələrdə kibertəhlükələr və risk faktorları

Sosial şəbəkələr məxfilik pozuntuları, kibertəhlükəsizlik hücumları, dezinformasiya, kibertəqib və süni intellekt vasitəsilə manipulyasiya kimi ciddi risklər yaradır. Bu təhdidlər cəmiyyətə, siyasətə və iqtisadiyyata mənfi təsir göstərir. Kiber cinayətkarlar sosial

şəbəkələrdən fişinq hücumları, zərərli proqramların yayılması və sosial mühəndislik hücumları üçün istifadə edirlər. Məsələn İyul 2020-də hakerlər Elon Musk, Barack Obama və Apple kimi yüksək səviyyəli Twitter hesablarını ələ keçirərək Bitcoin fırıldağı həyata keçirdilər və cəmi bir neçə saat ərzində 120,000 dollardan çox pul oğurladılar [1]. Bu hadisə sosial mühəndislik və hesab təhlükəsizliyinin zəif cəhətlərini üzə çıxardı.

Fişinq hücumları dünya üzrə fərdləri və təşkilatları hədəf alan ən yayılmış kibertəhlükələrdən biridir. Bu hücumlarda kibercinayətkarlar qurbanları şifrə və ya maliyyə məlumatları kimi həssas informasiyanı açıqlamağa məcbur etmək üçün aldadıcı e-poçtlar, mesajlar və ya veb-saytlardan istifadə edirlər. Fişinq hücumlarını həyata keçirənlər çox vaxt banklar, sosial media platformaları və ya hökumət qurumları kimi etibarlı təşkilatların adından çıxış edərək qurbanlarının etibarını qazanmağa çalışırlar. Ən çox yayılmış üsullardan biri olan e-poçt saxtalaşdırması zamanı hücumçular göndəricinin ünvanını saxtalaşdıraraq onu etibarlı göstərməyə çalışırlar. Spear fişinq isə fərdi məlumatlardan istifadə etməklə daha hədəfli və inandırıcı hücumlar təşkil edir.

Zərərli proqramlar ("malware" – "malicious software" söz birləşməsindən yaranıb) istifadəçilərin icazəsi olmadan kompüter sistemlərinə daxil olmaq, onları sıradan çıxarmaq və ya icazəsiz nəzarət əldə etmək üçün yaradılmış xüsusi proqramlardır. Bu cür proqramlar şəxsi istifadəçilərdən tutmuş iri korporasiyalara qədər müxtəlif hədəflərə hücum edə bilər və əsas məqsədləri arasında məlumat oğurluğu, sistemləri sıradan çıxarmaq, fidyə tələb etmək və ya kiber casusluq yer alır. Müasir dövrdə zərərli proqramların yayılmasında sosial media platformaları mühüm rol oynayır. Milyonlarla aktiv istifadəçisi olan bu platformalar kiberhücumçular üçün böyük bir hədəf kütləsi təmin edir. Fişinq hücumları, saxta linklər, zərərli reklamlar (malvertising) və saxta tətbiqlər sosial şəbəkələrdə zərərli proqramların yayılmasının ən çox istifadə olunan üsulları sırasındadır. Məsələn, Facebook, Instagram və X (keçmiş Twitter) kimi platformalarda hücumçular istifadəçiləri aldadaraq yoluxmuş linklərə klik etməyə sövq edir. Bu linklər adətən etibarlı bir şəxs və ya təşkilat adı altında göndərilir və istifadəçini saxta bir veb-sayta yönləndirir. Bu veb-saytda istifadəçinin cihazına avtomatik olaraq zərərli proqram yüklənir. Bununla yanaşı, WhatsApp və Telegram kimi mesajlaşma tətbiqləri də kiberhücumçular üçün effektiv vasitələrdən biridir. Hücumçular burada istifadəçilərə cəlbedici təkliflər, saxta kampaniyalar və ya təhlükəsizlik yeniləmələri adı altında zərərli proqramlar yüklətməyə çalışırlar. Həmçinin, sosial mediada yayılan saxta reklamlar istifadəçiləri yoluxmuş veb-saytlara yönləndirərək onların cihazlarına təhlükə yaradır.

Sosial şəbəkələrdə ən mühüm məsələlərdən biri istifadəçi məxfiliyinin qorunmasıdır. Sosial media platformaları geniş miqdarda şəxsi məlumat toplayır və bu məlumatlar korporasiyalar, reklamçılar və zərərli şəxslər tərəfindən sui-istifadə edilə bilər. Bu cür icazəsiz giriş şəxsiyyət oğurluğuna, məlumatların qanunsuz toplanmasına və nüfuzun zədələnməsinə səbəb ola bilər. Cambridge Analytica qalmaqalı təxminən 87 milyon Facebook istifadəçisinin şəxsi məlumatlarının onların razılığı olmadan toplandığını və siyasi reklam məqsədilə istifadə edildiyini ortaya çıxardı. Bu hadisə dünya miqyasında məxfilik və tənzimləyici nəzarət

məsələlərinə dair ciddi narahatlıqlar yaratdı və Avropa İttifaqında Ümumi Məlumatların Qorunması Qaydası (*General Data Protection Regulation* - GDPR) kimi daha sərt tənzimləmələrin qəbul edilməsinə səbəb oldu.

Sosial şəbəkələr dezinformasiyanın sürətli yayılmasına səbəb olaraq siyasi proseslərə, ictimai səhiyyəyə və ictimai sabitliyə ciddi təsir göstərir. Bu platformaların alqoritmləri sensasiyalı və emosional məzmunu prioritetləşdirir, nəticədə yalan məlumatlar daha geniş auditoriyaya çatır. Tədqiqatlar göstərir ki, saxta xəbərlər yeniliyi və psixoloji cəlbediciliyi səbəbindən doğru informasiyalardan daha sürətli yayılır [2]. Siyasi müstəvidə bu, seçkilərə müdaxilə və cəmiyyətin qütbləşməsinə, səhiyyədə isə peyvənd tərəddüdü və elmi əsassız müalicə üsullarının yayılmasına gətirib çıxarır [3]. Bundan əlavə, sosial media ekosistemində *əks-səda otaqları (echo chambers)* və *filtr qabarcıqları (filter bubbles)* fərqli baxışların yayılmasını məhdudlaşdıraraq dezinformasiyanın təsirini gücləndirir [4].

Kibertəqib və onlayn zorakılıq müasir dövrdə sosial və psixoloji problemlərdən birinə çevrilib. Anonimlik və onlayn ünsiyyətin inhibisiya effekti insanları real həyatda etməyəcəkləri aqressiv və dağıdıcı davranışlara sövq edir. Psixoloji təsirləri arasında narahatlıq, depressiya, özünəinamsızlıq və sosial təcrid kimi hallar mövcuddur. Kibertəqib məkan və zaman məhdudiyyətlərindən asılı olmadığından qurbanlar üçün daimi və qaçılmaz bir problem yaradır, onların akademik və peşəkar həyatına da mənfi təsir göstərir.

Süni intellektin (AI) sürətli inkişafı sosial şəbəkələrdə məzmunun yaradılması və manipulyasiyası üçün mürəkkəb metodlar təqdim edib. Bu texnologiyalar arasında deepfake texnologiyası xüsusilə seçilir, çünki onun vasitəsilə hiper-realist, lakin saxta videolar hazırlanır. Bu videolar tamaşaçıları aldadaraq ictimai fiqurların əslində demədiyi və etmədiyi şeyləri ifadə etdiyini göstərə bilər. Deepfake texnologiyası xüsusilə siyasi sahədə təhlükəlidir, çünki saxta məlumatların yayılması, ictimai rəyin manipulyasiyası və demokratik proseslərin pozulması üçün istifadə edilə bilər. Siyasi deepfake videolarının yaratdığı təhlükə təkcə seçki manipulyasiyası ilə məhdudlaşmır. Onlar medianın və demokratik institutların etibarlılığına xələl gətirir, vətəndaşların gerçək və yalan arasında fərq qoymasını çətinləşdirir. Bu problemlərin həlli üçün tədqiqatçılar avtomatik deepfake aşkarlama metodları inkişaf etdirir və süni intellektlə yaradılan dezinformasiyanın yayılmasını məhdudlaşdırmaq üçün daha sərt qanunların qəbul olunmasını təklif edirlər.

Sosial şəbəkə analizi və qraf nəzəriyyəsi ilə təhdidlərin aşkarlanması

SNA və qraf nəzəriyyəsi saxta xəbərlər, kibertəqib, onlayn zorakılıq və kibertəhlükəsizlik təhdidləri kimi problemlərin müəyyən edilməsi və qarşısının alınmasında vacib alətlərə çevrilmişdir. Bu analitik üsullar şəbəkə strukturlarını, istifadəçi qarşılıqlı əlaqələrini və məlumat axınını öyrənərək, zərərli fəaliyyətləri aşkarlamaq üçün məlumat əsaslı yanaşma təqdim edir. SNA bir şəbəkə daxilində obyektlər arasındakı münasibətləri öyrənən metodologiyadır. Sosial media kontekstində bu obyektlər (düyünlər, yəni istifadəçilər və ya

botlar) və aralarındakı əlaqələr (kənarlar, yəni mesajlar, paylaşımlar və ya izləmə əlaqələri) kimi təmsil olunur [5].

Sosial şəbəkə analizində təhdidlərin aşkarlanması üçün bir neçə əsas ölçü mövcuddur. *Dərəcə mərkəzliyi (degree centrality)* şəbəkədə ən çox əlaqəyə sahib və təsir gücü yüksək olan düyünləri müəyyən edir. *Aralıq mərkəzliyi (betweenness centrality)* məlumat axınında vasitəçi rolunu oynayan düyünləri aşkar edərək, dezinformasiya və bot şəbəkələrinin əsas yayıcılarını müəyyən etməyə kömək edir. *Yaxınlıq mərkəzliyi (closeness centrality)* isə məlumatın ən sürətli yayıldığı düyünləri göstərir və bu, saxta xəbərlərin yayılma mexanizmini öyrənmək üçün vacibdir. *İcma aşkarlanması (community detection)* isə oxşar davranış sərgiləyən istifadəçiləri qruplaşdıraraq bot şəbəkələri və koordinasiyalı dezinformasiya kampaniyalarının aşkarlanmasına imkan yaradır [6]. Bu ölçülər birlikdə tətbiq edildikdə, sosial şəbəkələrdə təhlükəli fəaliyyətlərin daha effektiv aşkarlanmasını təmin edir.

Saxta xəbərlər sosial mediada koordinasiyalı dezinformasiya kampaniyaları və botların dəstəklədiyi yayılma mexanizmləri vasitəsilə geniş yayılır. Sosial şəbəkə analizi və qraf nəzəriyyəsi saxta xəbərlərin aşkarlanmasında mühüm rol oynayır. İlk olaraq, məlumat axınlarının təhlili göstərir ki, saxta xəbərlər adətən "əks-səda otaqları" daxilində sürətlə yayılır, halbuki həqiqi xəbərlər daha müxtəlif auditoriyaya malik orqanik paylaşım nümunəsi sərgiləyir. Digər tərəfdən, koordinasiyalı bot şəbəkələrinin aşkarlanması saxta məlumatların yayılmasını öyrənmək üçün əhəmiyyətlidir, çünki bot hesablar çox sıx əlaqəli qruplar yaradaraq insan istifadəçilərdən fərqli davranış nümayiş etdirir. Bundan əlavə, məlumatın əsas yayıcılarının müəyyən edilməsi də vacibdir, çünki *aralıq mərkəzliyi (betweenness centrality)* yüksək olan düyünlər çox vaxt dezinformasiyanın əsas yayılma nöqtələri olur. Tədqiqatçılar qraf strukturlarını təhlil edərək və maşın öyrənməsi modellərindən istifadə edərək saxta xəbər mənbələrini təsnif edir və onların etibarlılığını qiymətləndirirlər. Bu yanaşmalar saxta xəbərlərin yayılma yollarını anlamağa və onların qarşısını almağa imkan yaradır.

Sosial şəbəkə analizi və qraf nəzəriyyəsi kibertəqib, nifrət nitqi və koordinasiyalı zorakılıq kampaniyalarının aşkarlanmasında mühüm rol oynayır. Araşdırmalar göstərir ki, təqib şəbəkələri yüksək klasterləşmə və modulluluq nümayiş etdirir, burada bir neçə istifadəçi koordinasiyalı şəkildə müəyyən bir fərdi hədəfə alır. Toksik istifadəçi aşkarlanması üçün isə mərkəzlik ölçüləri və sentiment analizi birləşdirilir, çünki təcavüzkarlar adətən çoxsaylı mənfi qarşılıqlı əlaqələrdə iştirak edirlər. Bundan başqa Avtomatlaşdırılmış moderasiya sistemləri SNA-dan istifadə edərək təcavüzkar davranışları izləyir və yüksək riskli icmaları müəyyən edir. Daha da inkişaf etmiş metodlar arasında maşın öyrənməsi modelləri ilə SNA-nın inteqrasiyası yer alır ki, bu da real vaxt rejimində təhdidlərin aşkarlanmasını və onların qarşısının alınmasını mümkün edir.

Kiber cinayətkarlar sosial şəbəkələrdən fişinq hücumları, zərərli proqramların yayılması və botnet hücumları üçün geniş istifadə edirlər. Sosial şəbəkə analizi və qraf nəzəriyyəsi bu hücumların aşkarlanmasında effektiv üsullardan biri sayılır. İlk olaraq, anomal istifadəçi davranışlarının müəyyən edilməsi bot və saxta hesabların aşkarlanmasına kömək edir. Bu

hesablar aşağı qarşılıqlı əlaqə dərəcəsinə, qeyri-təbii fəaliyyət sıçrayışlarına və nizamsız davranış nümunələrinə malik olur. Belə istifadəçilər bir-birilərini sürətlə izləyir, məzmunu avtomatlaşdırılmış şəkildə paylaşır və insan davranışından fərqli fəaliyyət nümayiş etdirir. Botnetlərin struktur analizi onların aşkarlanması üçün vacibdir, çünki bu zərərli şəbəkələr xüsusi qruplaşmış qraf strukturları yaradır və fəaliyyətləri koordinasiyalı şəkildə idarə olunur. Botnetlər vasitəsilə kütləvi saxta məlumat yayımı, DDoS hücumları və fişinq kampaniyaları həyata keçirilir. Qraf nəzəriyyəsinə əsaslanan analizlər botnetlərin unikal qruplaşmalarını aşkar edərək onların fəaliyyətini izləməyə imkan yaradır. Süni intellekt əsaslı anomaliya aşkarlama alqoritmlərinin SNA ilə inteqrasiyası real vaxt rejimində təhdidlərin müəyyən edilməsi və qarşısının alınmasını təmin edərək kibertəhlükəsizlik strategiyalarını gücləndirir.

Müasir dövrdə sosial şəbəkələr informasiya mübadiləsinin ən güclü vasitələrindən birinə çevrilsə də, saxta xəbərlər, kibertəqib, onlayn zorakılıq və kibertəhlükəsizlik təhdidləri kimi ciddi problemlərlə üzləşir. Bu tədqiqat göstərdi ki, Sosial şəbəkə analizi və qraf nəzəriyyəsi bu təhdidlərin aşkarlanması və aradan qaldırılması üçün mühüm alətlərdir. Saxta məlumatların məlumat axınları, əlaqə strukturları və sosial şəbəkə dinamikası üzərindən təhlili, dezinformasiya kampaniyalarının əsas yayılma mənbələrini və manipulyativ aktorlarını müəyyən etməyə imkan yaradır.

Bundan əlavə, SNA və qraf əsaslı yanaşmalar kibertəhlükəsizlik sahəsində də güclü vasitələr kimi çıxış edir. Botnet şəbəkələrinin, fişinq hücumlarının və zərərli proqramların struktur və fəaliyyət modellərinin analizi onların daha erkən aşkarlanmasını və neytrallaşdırılmasını təmin edir. Xüsusilə süni intellekt əsaslı anomalik aşkarlama sistemlərinin inteqrasiyası, təhdidlərin real vaxt rejimində müəyyən edilməsinə və qabaqlayıcı tədbirlərin görülməsinə şərait yaradır. Lakin SNA-nın tətbiqi məlumat məxfiliyi, kiber cinayətkarların yeni deteksiya metodlarına adaptasiyası və böyük verilənlərin emalı üçün yüksək hesablama gücü tələbi kimi bir sıra problemlərlə qarşılaşır. Buna baxmayaraq, qraf neyron şəbəkələri (GNN), federativ öyrənmə və izah edilə bilən süni intellekt (XAI) kimi innovativ texnologiyalar gələcəkdə bu maneələri aradan qaldıraraq təhlükəsizlik sistemlərinin daha şəffaf, effektiv və etik cəhətdən dayanıqlı olmasına imkan verəcəkdir.

Nəticə etibarilə, SNA və qraf nəzəriyyəsinin kibertəhlükəsizlik və sosial media təhlili sahələrində rolu artmaqda davam edir. Gələcək tədqiqatlar bu yanaşmaların təkmilləşdirilməsi, etik çərçivələrin gücləndirilməsi və yeni texnologiyalarla inteqrasiyası üzərində fokuslanmalıdır. Belə inkişaflar, sosial platformaları daha təhlükəsiz, etibarlı və manipulyasiyadan qorunmuş bir mühitə çevirmək üçün əsas addımlardan biri olacaqdır.

Ədəbiyyat

1. Bloomberg. (2020). Twitter accounts of Biden, Obama and other prominent figures hacked. Irish Times. Retrieved from https://www.irishtimes.com/news/world/us/twitter-accountsof-biden-obama-and-other-prominent-figures-hacked-1.4305567
2. Vosoughi, S., Roy, D. & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146-1151.
3. Bovet, A., Makse, H. A. (2019). Influence of fake news in Twitter during the 2016 US presidential election. *Nature Communications, 10*(1), 7. https://doi.org/10.1038/s41467-018-07761-2
4. Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W. & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences, 118*(9), e2023301118. https://doi.org/10.1073/pnas.2023301118
5. Wasserman, S., Faust, K. (1994). *Social Network Analysis: Methods and Applications*. Cambridge University Press. https://doi.org/10.1017/CBO9780511815478
6. Fortunato, S. (2010). Community detection in graphs. *Physics Reports*, 486(3-5), 75-174.

SOCIAL NETWORK ANALYSIS IN CYBERSECURITY: IDENTIFICATION OF RISKS AND THREATS

N.A. Hasanova, E.A. Samadzade
Azerbaijan University, Jeyhun Hajibeyli, 71, Baku, Azerbaijan

Abstract. Social Network Analysis (SNA) has become an essential tool in the field of cybersecurity as an approach based on the analysis of relationships within a network. This paper explores graph metrics such as *betweenness*, *degree* and *closeness centrality*, as well as *community detection* methods, for the purpose of identifying cyber threats. The main objective of the research is to assess the potential for identifying and preventing cyber threats by analyzing the structures of social networks.

Keywords: Social Network Analysis, cybersecurity, cyber Threats, graph metrics, graph theory, social platforms.