Sosial Media Resurslarında Gizli Mütəşəkkil Kibercinayətkar Qrupların Aşkarlanması Metodu

Günay Iskəndərli
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
gunayniftali@gmail.com

***Xülasə*— Məqalədə sosial media mühitində gizli mütəşəkkil qrupların aşkarlanması üçün zaman, struktur və davranış faktorlarını birgə nəzərə alan hibrid dinamik qraf neyron şəbəkə modeli təklif olunur. Modeldə istifadəçilər aktivlik, sentiment, əlaqə dərəcəsi kimi göstəricilərlə təsvir olunur. İstifadəçilər arasındakı əlaqələr isə qarşılıqlı fəaliyyət və zaman uyğunluğu əsasında çəkili qraf modeli ilə müəyyən edilir, gizli davranış xüsusiyyətləri öyrənilir, daha sonra klasterləşdirmə vasitəsilə potensial gizli qruplar aşkarlanır. Təklif olunan metod sosial media analizinin dəqiqliyini artırır və kibercinayətkarlıqla mübarizə məqsədilə qərar qəbuletmə prosesinin dəstəklənməsi üçün perspektivli yanaşma təqdim edir.**

***Açar sözlər*— Sosial media analizi; kibercinayətkarlıq; qraf neyron şəbəkələri; klasterləşmə; kibertəhlükəsizlik.**

I. GİRİŞ

Son illərdə informasiya-kommunikasiya texnologiyalarının (İKT) sürətli inkişafı nəticəsində sosial media gündəlik həyatın ayrılmaz hissəsinə çevrilmişdir. Xüsusilə Facebook, Instagram, Twitter və digər platformalar insanların ünsiyyət qurma, məlumat paylaşma və ictimai proseslərdə iştirak etmə formalarını köklü şəkildə dəyişmişdir. Bu dəyişikliklər təkcə sosial münasibətlərə deyil, həm də iqtisadi, siyasi və təhlükəsizlik sahələrinə ciddi təsir göstərmişdir [3, 8].

Azərbaycan Respublikasında da rəqəmsallaşma siyasəti dövlət səviyyəsində prioritet istiqamətlərdən biridir. Rəqəmsal hökumət (e-gov) xidmətlərinin genişlənməsi, rəqəmsal idarəetmə sistemlərinin tətbiqi və informasiya təhlükəsizliyinin gücləndirilməsi ölkədə müasir İKT infrastrukturunun formalaşmasına təkan vermişdir. Bununla yanaşı, sosial şəbəkələrin geniş istifadəsi yeni imkanlarla yanaşı, müəyyən təhlükəsizlik riskləri yaratmışdır.

Müasir dövrdə kibermühitdə fəaliyyət göstərən mütəşəkkil qruplar sosial media platformalarından gizli əlaqələrin koordinasiyası üçün istifadə edirlər. Bu cür qrupların aşkarlanması hüquq-mühafizə orqanları və təhlükəsizlik strukturları üçün mühüm əhəmiyyət kəsb edir. Çünki belə qruplar çox vaxt açıq şəkildə deyil, dolayı kommunikasiya və gizli davranış nümunələri vasitəsilə fəaliyyət göstərirlər.

Mövcud tədqiqatlarda sosial media analizində əsasən iki yanaşma geniş istifadə olunur: sosial şəbəkə analizi və mətn analizi (Text Mining) [3, 4]. Lakin bu yanaşmaların əksəriyyəti ya yalnız istifadəçilər arasındakı struktur əlaqələri, ya da yalnız mesaj məzmununu nəzərə alır. Bu isə mürəkkəb və dinamik sosial mühitlərdə gizli mütəşəkkil qrupların tam şəkildə aşkarlanmasını çətinləşdirir.

Real sosial şəbəkələr dinamik struktura malikdir və istifadəçi davranışları zamanla dəyişir [8]. İstifadəçilərin aktivlik səviyyəsi, emosional ifadələri, qarşılıqlı əlaqə intensivliyi və zaman sinxronluğu kimi faktorlar gizli qrupların müəyyən edilməsində mühüm rol oynayır. Məsələn, eyni zaman intervalında oxşar fəaliyyət göstərən və oxşar emosional məzmun paylaşan istifadəçilər arasında daha güclü əlaqələrin olması ehtimalı yüksəkdir [6, 11].

Bu tədqiqat işində sosial media mühitində gizli mütəşəkkil kibercinayətkar qrupların aşkarlanması üçün zaman, struktur və davranış faktorlarını birgə nəzərə alan kompleks yanaşma təklif olunur. Təklif olunan model Azərbaycan Respublikasında formalaşan rəqəmsal informasiya mühiti və artan kibertəhlükəsizlik tələbləri fonunda xüsusilə aktualdır. Çünki rəqəmsal dövlət sistemlərinin genişlənməsi ilə paralel olaraq rəqəmsal məkanda təhlükəsizlik məsələlərinin elmi əsaslarla araşdırılması vacib hala gəlmişdir.

Təklif olunan metod sosial şəbəkəni dinamik qraf kimi nəzərdən keçirir və istifadəçi fəaliyyətini zaman kontekstində təhlil edir. İstifadəçilər arasındakı əlaqələr yalnız struktur göstəricilər deyil, həm də davranış oxşarlığı, emosional uyğunluq və zaman sinxronluğu kimi çoxölçülü faktorlar əsasında qiymətləndirilir. Daha sonra GCN vasitəsilə istifadəçilərin gizli davranış xüsusiyyətləri öyrənilir və klasterləşmə üsulu ilə potensial gizli qruplar aşkarlanır.

Beləliklə, təqdim olunan yanaşma sosial media analizində daha dəqiq və real nəticələrin əldə olunmasına imkan yaradır və kibercinayətkarlıqla mübarizə sahəsində tətbiq oluna biləcək effektiv bir metodoloji çərçivə formalaşdırır. İrəli sürülən yanaşmalar nəzərə alınaraq, bu tezis aşağıdakı bölmələr üzrə strukturlaşdırılmışdır: İkinci bölmədə sosial media mühitində gizli mütəşəkkil kibercinayətkar qrupların aşkarlanması sahəsində mövcud elmi yanaşmalar və əlaqəli tədqiqatlar təhlil edilmişdir. Üçüncü bölmədə təklif olunan metodun nəzəri əsasları, sosial şəbəkənin qurulması, zaman və davranış faktorlarının modelləşdirilməsi ətraflı şəkildə izah olunmuşdur. Dördüncü bölmədə isə aparılan tədqiqatın nəticələri ümumiləşdirilmiş və əldə olunan nəticələrin praktik əhəmiyyəti qiymətləndirilmişdir.

II. ƏLAQƏLİ İŞLƏR

Sosial media mühitində gizli mütəşəkkil kibercinayətkar qrupların aşkarlanması sahəsi son illərdə intensiv şəkildə tədqiq olunur. Bu istiqamətdə aparılan tədqiqatlar əsasən sosial şəbəkə analizi, Text Mining və bu iki yanaşmanın inteqrasiyasına əsaslanır.

Sosial şəbəkə analizi sahəsində aparılan ilkin işlərdə

DOI: 10.25045/forensic.gov.2026.10

istifadəçilər arasındakı əlaqələr qraf strukturu kimi modelləşdirilərək icma aşkarlanması (community detection) metodları tətbiq edilmişdir. Məsələn, [1] və [2]-də təklif olunan metodlar şəbəkə daxilində sıx əlaqəli qrupların müəyyən edilməsinə imkan verir. Bununla yanaşı, Wasserman və Faust sosial şəbəkələrin struktur analizinin nəzəri əsaslarını təqdim etmişdir [3]. Lakin bu yanaşmalar əsasən struktur məlumatlara əsaslandığı üçün gizli və ya semantik əlaqəli qrupların aşkarlanmasında məhdudiyyətlərə malikdir.

Digər tərəfdən, mətn analizi və təbii dil emalı metodları sosial media məzmununun analizində geniş istifadə olunur. Blei və digərləri tərəfindən təklif edilən Latent Dirichlet Allocation modeli mövzu modelləşdirmə sahəsində geniş tətbiq olunmuşdur [4]. Bu yanaşma istifadəçi mesajlarından gizli mövzuların çıxarılmasına imkan verir. Eyni zamanda, Chen və digərləri terrorizm və ekstremizm fəaliyyətinin aşkarlanmasında text mining metodlarının tətbiqini araşdırmışdır [5].

Daha sonrakı tədqiqatlar göstərmişdir ki, yalnız mətn və ya yalnız struktur analiz kifayət etmir. Bu səbəbdən hibrid yanaşmalar – xüsusilə məzmun əsaslı sosial şəbəkə analizi (content-based social network analysis) metodları inkişaf etdirilmişdir. Bu yanaşma həm istifadəçilər arasındakı əlaqəni, həm də onların paylaşdıqları məzmunu birlikdə analiz etməyə imkan verir. Zhou və digərləri kriminal şəbəkələrin aşkarlanmasında sosial əlaqələr və düyünlərə məxsus atribut xüsusiyyətlərinin birgə istifadəsinin effektivliyini göstərmişdir [6].

Bundan əlavə, maşın öyrənməsi və dərin öyrənmə əsaslı metodlar da geniş yayılmışdır. Xüsusilə qraf neyron şəbəkələri (Graph Neural Networks – GNN) sosial şəbəkələrdə həm struktur, həm də məzmun xüsusiyyətlərini öyrənmək üçün istifadə olunur [7]. Bu yanaşmalar böyük həcmli məlumatların avtomatik emalını təmin edərək gizli qrupların daha dəqiq aşkarlanmasına şərait yaradır.

Kumar və digərləri dinamik sosial şəbəkələrin analizini apararaq koordinasiyalı fəaliyyətin müəyyən edilməsini təklif etmişdir [8]. Bu yanaşma xüsusilə qısa müddətli kampaniyalar və koordinasiyalı hücumların aşkarlanmasında effektivdir.

Mövcud tədqiqatların analizi göstərir ki, sosial media mühitində gizli kibercinayətkar qrupların aşkarlanması sahəsində müxtəlif yanaşmalar mövcud olsa da, bu metodların əksəriyyəti struktur, məzmun və zaman faktorlarını kompleks şəkildə nəzərə almır. Bu məhdudiyyətləri aradan qaldırmaq məqsədilə növbəti bölmədə zaman, struktur və davranış xüsusiyyətlərini inteqrasiya edən hibrid qraf əsaslı metod təqdim olunur.

III. TƏKLİF OLUNAN METOD

Əvvəlki bölmələrdə sosial media mühitində gizli mütəşəkkil kibercinayətkar qrupların aşkarlanması sahəsində mövcud yanaşmalar və onların məhdudiyyətləri təhlil edilmişdir. Bu məhdudiyyətləri nəzərə alaraq, bu tədqiqatda zaman, struktur və davranış faktorlarını eyni anda inteqrasiya edən hibrid qraf əsaslı metod təklif olunur. Metodun əsas məqsədi dinamik sosial şəbəkələrdə koordinasiyalı fəaliyyət göstərən istifadəçi qruplarını daha dəqiq şəkildə müəyyən etməkdir.

Təklif olunan yanaşmanın əsas ideyası ondan ibarətdir ki, gizli şəkildə təşkilatlanmış qruplar yalnız istifadəçilər arasındakı struktur əlaqələrlə deyil, eyni zamanda onların fəaliyyət zamanlarının sinxronluğu, davranış oxşarlığı və emosional ton (sentiment) uyğunluğu ilə xarakterizə olunur [6, 8, 11]. Buna görə də sosial şəbəkə statik bir qraf kimi deyil, zamanla dəyişən dinamik sistem kimi modelləşdirilir və istifadəçi davranışları zaman kontekstində analiz edilir.

Bu məqsədlə sosial media mühitində müşahidə olunan məlumatlar zaman intervallarına bölünərək hər bir interval üçün ayrıca sosial şəbəkə qrafı qurulur. Daha sonra istifadəçilər çoxölçülü xüsusiyyət vektorları ilə təsvir edilir, onlar arasındakı əlaqələr isə çəkili qonşuluq matrisi şəklində formalaşdırılır. Bu struktur üzərində GCN tətbiq edilərək istifadəçilərin gizli davranış xüsusiyyətləri öyrənilir və nəticədə klasterləşmə üsulu ilə potensial koordinasiyalı qruplar müəyyən edilir . Təklif olunan metod aşağıdakı mərhələlərdən ibarətdir:

1) Verilənlərin toplanması və şəbəkənin qurulması
2) Zaman üzrə davranışın analizi
3) Xüsusiyyət matrisi və əlaqə gücünün hesablanması
4) GCN vasitəsilə öyrənmə
5) Klasterləşmə və gizli qrupların aşkarlanması

1) Verilənlərin toplanması və şəbəkənin qurulması: Sosial media mühitində müşahidə olunan zaman anları aşağıdakı kimi təyin olunur:

$$T = \{t_1, t_2, \dots, t_K\} \quad (1)$$

burada $K -$müşahidə olunan diskret zaman anlarının ümumi sayıdır. Hər bir zaman anında paylaşılmış postlar çoxluğu aşağıdakı kimi təyin olunur:

$$P(t_k) = \{p_1(t_k), p_2(t_k), \dots, p_{m_k}(t_k)\}, k = 1,2,\dots,K \quad (2)$$

burada $P(t_k) - t_k$ zaman anında paylaşılan bütün postlar çoxluğu, $m_k - t_k$ zaman anında paylaşılan postların sayıdır. Hər posta şərh yazan istifadəçilər çoxluğu aşağıdakı kimi ifadə olunur:

$$U_r(t_k) = \{u_{r1}, u_{r2}, \dots, u_{rn_k}\}, r = 1,2,\dots,m_k, k = 1,2,\dots,K \quad (3)$$

burada $U_r(t_k) - t_k$ zaman anında r -ci posta şərh yazan istifadəçilər çoxluğu, $n_k -$istifadəçilərin sayıdır. Beləliklə, hər bir zaman anı üçün aktiv istifadəçilər çoxluğu aşağıdakı kimi müəyyən edilir:

$$U(t_k) = \cup_{r=1}^{m_i} U_r(t_k), k = 1,2,\dots,K \quad (4)$$

2) Zaman üzrə davranışın analizi: Təsadüfi istifadəçiləri mütəşəkkil qruplardan ayırmaq üçün aşağıdakı düsturdan istifadə olunur:

$$U^* = \bigcap_{k=1}^{K} U(t_k) \quad (5)$$

$$|U^*| = N \quad (6)$$

burada $N -$ mütəşəkkil qrupa daxil olan istifadəçilərin sayıdır. Bu ifadə ardıcıl zaman intervallarında aktiv olan istifadəçiləri müəyyən edir. Bu çoxluq potensial mütəşəkkil qrupların əsas iştirakçılarını (stabil istifadəçiləri) ifadə edir.

Mütəşəkkil qrupun üzvləri müəyyən edildikdən sonra bu istifadəçilər arasında qarşılıqlı əlaqələri analiz etmək məqsədilə şəbəkə modeli qurulur. Bu məqsədlə $G = (V, E)$ qrafı təyin edilir. Burada $V = U^* -$mütəşəkkil qrupun stabil istifadəçilər çoxluğunu, E isə istifadəçilər arasındakı əlaqələri ifadə edir. İki istifadəçi arasında əlaqə eyni posta şərh yazdıqda, bir-birinə cavab verdikdə və ya digər sosial qarşılıqlı əlaqələr olduqda formalaşır. Beləliklə, qurulan şəbəkə potensial mütəşəkkil davranış nümunələrinin struktur analizinə imkan yaradır.

3) Xüsusiyyət matrisi və əlaqə gücünün hesablanması. Qurulmuş şəbəkə modeli istifadəçilər arasındakı struktur əlaqələri əks etdirsə də, mütəşəkkil davranışın daha dərindən təhlili üçün hər bir istifadəçinin fərdi xüsusiyyətlərinin və qarşılıqlı əlaqələrinin kəmiyyət baxımından qiymətləndirilməsi zəruridir. Bu məqsədlə istifadəçilər çoxölçülü xüsusiyyətlər vektoru ilə təsvir olunur və onlar arasındakı əlaqə gücü hesablanır. Beləliklə, hər bir istifadəçi aşağıdakı xüsusiyyətlər vektoru ilə xarakterizə olunur:

4)

$$u_i^* = [a_i, s_i, e_i], i = 1,2, \dots, N \quad (7)$$

burada $u_i^* -$ mütəşəkkil qrupa daxil olan $i -$ ci istifadəçinin xüsusiyyət vektoru, $a_i -$istifadəçinin aktivliyi, $s_i -$ sentiment göstəricisi, $e_i -$ əlaqə dərəcəsidir. Qeyd olunan xüsusiyyətlər aşağıdakı kimi müəyyən edilir:

$$a_i = \frac{1}{K}\sum_{k=1}^{K} n_i(t_k) \quad (8)$$

$$s_i = \frac{1}{n_i}\sum_{r=1}^{n_i} score(p_r^i) \quad (9)$$

$$e_i = \frac{\left|\left\{u_j^* : (u_i^*, u_j^*) \in E\right\}\right|}{N-1} \quad (10)$$

burada $n_i(t_k) - i -$ ci istifadəçinin $k -$ cı zaman anında paylaşdığı postların sayı, $score(p_r^i) - i -$ ci istifadəçinin paylaşdığı $r -$ ci postun sentiment analizinə əsasən əldə olunmuş qiyməti, $n_i - i -$ci istifadəçinin paylaşdığı postların ümumi sayı, $e_i - i -$ci istifadəçinin şəbəkədəki əlaqələrinin sayıdır.

Beləliklə, hər bir istifadəçi üçün əldə olunan xüsusiyyətlər vektor şəklində təqdim edilərək birləşdirilir və nəticədə istifadəçiləri təsvir edən xüsusiyyət matrisi formalaşdırılır:

$$X = \begin{bmatrix} u_1^* \\ u_2^* \\ \vdots \\ u_N^* \end{bmatrix} \quad (11)$$

Bu vektorlardan istifadə edərək istifadəçilər arasında əlaqənin gücü tapılır. Bunun üçün kosinus metrikasından istifadə olunması təklif olunur. İstifadəçilər arasındakı əlaqələr çəkili qonşuluq matrisi şəklində təqdim olunur:

$$A = [w_{ij}] \quad (12)$$

Burada $w_{ij} -$ istifadəçilər arasındakı əlaqənin gücünü ifadə edir və aşağıdakı kimi hesablanır:

$$w_{ij} = \frac{u_i^* \cdot u_j^*}{\|u_i^*\| \cdot \|u_j^*\|} \quad (13)$$

5) GCN vasitəsilə öyrənmə: Xüsusiyyət matrisi və əlaqə matrisi istifadəçilər haqqında ilkin təsviri məlumat versə də, bu məlumatlar şəbəkə strukturunun təsirini tam şəkildə əks etdirmir. Mütəşəkkil davranışın əsas xüsusiyyətlərindən biri istifadəçilər arasındakı qarşılıqlı əlaqələrin və qrup dinamikasının mühüm rol oynamasıdır. Bu səbəbdən, həm istifadəçi xüsusiyyətlərini, həm də şəbəkə strukturunu birlikdə nəzərə almaq üçün GCN modelindən istifadə olunur. GCN modeli hər bir istifadəçinin xüsusiyyətlərini onun qonşularının xüsusiyyətləri ilə aqreqasiya edərək daha zəngin və kontekstual vektor (embedding) formalaşdırır. Nəticədə əldə olunan bu vektorlar istifadəçilər arasında gizli əlaqələri və mütəşəkkil davranış nümunələrini daha effektiv şəkildə aşkar etməyə imkan verir. Bu yanaşmaya əsasən, xüsusiyyət matrisi X və əlaqə matrisi A giriş verilənləri kimi qəbul edilərək GCN modeli tətbiq olunur [9]:

$$H^{(l+1)} = \sigma(\tilde{D}^{-1/2} \cdot \tilde{A} \cdot \tilde{D}^{-1/2} \cdot H^{(l)} \cdot W^{(l)}) \quad (14)$$

burada $H^{(l)} - l -$ci layın xüsusiyyət matrisi olub, $H^{(0)} = X$, $\tilde{A} = A + I$, $\tilde{D} -$dərəcə matrisi, $W^{(l)} -$öyrənilən çəkilər,$\sigma -$ aktivasiya funksiyasıdır.

Qeyd edək ki, aktivasiya funksiyası kimi ReLU istifadə olunmuşdur. İstifadəçilər arasındakı əlaqə güclərini nəzərə alan çəkili dərəcə matrisi $\widetilde{D} -$diaqonal matris olub aşağıdakı kimi hesablanır:

$$\tilde{D} = diag(d_1, d_2, \dots, d_N) \quad (15)$$

burada hər bir istifadəçinin ümumi əlaqə dərəcəsi, qonşuluq matrisindəki müvafiq sətrin elementlərinin cəminə bərabərdir:

$$d_i = \sum_{j=1}^{N} w_{ij}, i = 1,2, \dots, N \quad (16)$$

burada w_{ij} - (11) düsturu ilə hesablanmış i və j istifadəçiləri arasındakı əlaqənin gücüdür. Son layın çıxışı aşağıdakı kimi ifadə olunur:

$$Z = H^{(L)} \quad (17)$$

Bu vektorlar istifadəçilərin gizli davranış xüsusiyyətlərini əks etdirir.

6) Klasterləşmə və gizli qrupların aşkarlanması: Əldə olunan Z vektorları əsasında istifadəçilər K-means alqoritmi vasitəsilə klasterlərə bölünür [10]:

$$C = \{C_1, C_2, .., C_M\} \quad (18)$$

burada M −klasterlərin sayıdır. Klasterləşmə nəticəsində əldə olunan qruplar potensial mütəşəkkil istifadəçi qrupları kimi nəzərdən keçirilir.

Bu qrupların həqiqətən koordinasiyalı fəaliyyət göstərib-göstərmədiyini müəyyən etmək üçün növbəti mərhələlərdə onların daxili strukturu və davranış xüsusiyyətləri əlavə olaraq təhlil oluna bilər. Bu məqsədlə klaster daxilində əlaqə sıxlığı, zaman üzrə fəaliyyət sinxronluğu, istifadəçilərin sentiment uyğunluğu və stabil istifadəçilərin üstünlük təşkil etməsi kimi faktorlar qiymətləndirilə bilər.

Bu yanaşma sosial media mühitində istifadəçi davranışlarını çoxölçülü şəkildə təhlil etməyə və potensial koordinasiyalı qrupların daha dəqiq müəyyən edilməsinə imkan yaradır. Zaman faktoru, əlaqə strukturu və məzmun xüsusiyyətlərinin birgə nəzərə alınması metodun genişləndirilməsi və real tətbiqlərdə effektivliyinin artırılması üçün perspektiv istiqamət kimi çıxış edir.

NƏTİCƏ

Bu tədqiqatda sosial media mühitində gizli və potensial mütəşəkkil kibercinayətkar qrupların aşkarlanması üçün zaman, struktur və davranış faktorlarını inteqrasiya edən hibrid qraf əsaslı yanaşma təklif edilmişdir. Təklif olunan model sosial şəbəkələri dinamik sistem kimi təsvir edərək istifadəçi fəaliyyətlərinin çoxölçülü şəkildə təhlilinə imkan verir [7,9].

Bu yanaşmada istifadəçilər arasındakı əlaqələr yalnız struktur göstəricilər əsasında deyil, həm də davranış oxşarlığı və zaman üzrə aktivlik xüsusiyyətləri nəzərə alınmaqla modelləşdirilmişdir. GCN vasitəsilə istifadəçilərin gizli xüsusiyyətləri öyrənilmiş və bu xüsusiyyətlər əsasında klasterləşmə tətbiq edilərək oxşar davranış nümayiş etdirən istifadəçi qrupları müəyyən edilmişdir [8].

Əldə olunan klasterlər potensial koordinasiyalı qruplar kimi nəzərdən keçirilir. Bu qrupların həqiqətən mütəşəkkil olub-olmadığının daha dəqiq müəyyən edilməsi üçün onların daxili struktur və davranış xüsusiyyətlərinin — əlaqə sıxlığı, zaman sinxronluğu, məzmun uyğunluğu və aktivlik sabitliyi kimi faktorların — əlavə təhlili gələcək tədqiqat istiqaməti kimi təklif olunur.

ƏDƏBİYYAT

[1] M. E. J. Newman, "The structure and function of complex networks," SIAM Review, vol. 45, no. 2, pp. 167–256, 2003.

[2] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks," Proc. Natl. Acad. Sci., vol. 99, no. 12, pp. 7821–7826, 2002.

[3] S. Wasserman and K. Faust, Social Network Analysis: Methods and Applications. Cambridge, U.K.: Cambridge Univ. Press, 1994.(kitab olduguna gore duzgun yazilib)

[4] D. M. Blei, A. Y. Ng and M. I. Jordan, "Latent Dirichlet Allocation," J. Mach. Learn. Res., vol. 3, pp. 993–1022, 2003.

[5] H. Chen, E. Reid, J. Sinai, A. Silke and B. Ganor, Terrorism Informatics: Knowledge Management and Data Mining for Homeland Security. New York, NY, USA: Springer, 2008.(kitab olduguna gore duzgun yazilib)

[6] Y. Zhou, J. Qin, H. Chen, M. Chau and E. Reid, "Analyzing the structure of dark networks," IEEE Intell. Syst., vol. 20, no. 5, pp. 33–41, 2005.

[7] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang and P. S. Yu, "A comprehensive survey on graph neural networks," IEEE Trans. Neural Netw. Learn. Syst., vol. 32, no. 1, pp. 4–24, Jan. 2021.

[8] R. Kumar, J. Novak and A. Tomkins, "Structure and evolution of online social networks," in Link Mining: Models, Algorithms, and Applications, P. S. Yu, J. Han and C. Faloutsos, Eds. New York, NY, USA: Springer, 2010, pp. 337–357.

[9] A. Shen and K. P. Chow, "Community detection framework using deep learning in social media analysis," Applied Sciences, vol. 14, no. 3, pp. 1–19, 2024.

[10] P. Kim and S. Kim, "Detecting overlapping and hierarchical communities in complex network using interaction-based edge clustering," Physica A: Statistical Mechanics and its Applications, vol. 417, pp. 46–56, 2015.

[11] M. Dhilber and S. D. Bhavani, "Community detection in social networks using deep learning," in Proc. 16th Int. Conf. Distributed Computing and Internet Technology (ICDCIT), Bhubaneswar, India, Jan. 2020, pp. 241–250.

A Method for Detecting Hidden Organized Cybercriminal Groups in Social Media

Gunay Iskandarli
Institute of Information Technology, Baku, Azerbaijan
gunayniftali@gmail.com

Abstract- This paper proposes a hybrid dynamic graph neural network model that jointly considers temporal, structural, and behavioral factors to detect hidden organized groups in social media environments. In this model, users are characterized by features such as activity, sentiment, and connection degree. Relationships between users are established via a weighted graph model based on interaction and temporal alignment, enabling the learning of latent behavioral characteristics and the detection of potential hidden groups through clustering. The proposed method yields more precise results in social media analysis and serves as an effective tool for combating cybercrime.

Keywords- social media analysis; cybercrime; graph neural networks; clustering; cybersecurity.